HUMAN RELIABILITY AND SHIP STABILITY

by:
Robert D.G. Webb Ph.D.
Tabbeus M. Lamoureux M.Sc.

Humansystems Incorporated
111 Farquhar St., 2nd floor
Guelph, ON N1H 3N4

HSI® Project Manager:
Kim Iwasa-Madge
(519) 836 5911

PWGSC Contract No. W7711-017747/001/TOR
Call-Up 7747-14

On behalf of
DEPARTMENT OF NATIONAL DEFENCE

as represented by
Defence Research and Development Canada
1133 Sheppard Avenue West
Toronto, Ontario, Canada
M3M 3B9

DND Technical Authority
LtCdr Patrick Carnie, RCNC
DMSS 2-2
(819) 997-2268

July 4, 2003

© HER MAJESTY THE QUEEN IN RIGHT OF CANADA (2003)
as represented by the Minister of National Defense

© SA MAJESTE LA REINE EN DROIT DUE CANADA (2003)
Defense Nationale Canada

ABSTRACT

This report briefly reviews ship stability and capsize issues, risk assessment, and Human Factors issues related to risk of capsize during design and operation of warships. A generic approach to Human Reliability Analysis (based on Kirwan 1994) is described in some detail. Based on this approach, a four part two year plan is proposed to establish and apply a Human Reliability Analysis approach to estimate Human Factors risks related to warship capsize and management of stability. This work was conducted under Standing offer W7711-017747/001/TOR, Call-up 7747-14 with DRDC-Toronto and submitted in July 2003.

Executive Summary

This report was prepared for the Canadian Department of National Defence (DMSS 2-2). The purpose of the report was to draft a strategic plan to review methods to identify and quantify the impact of human reliability on capsize probability.

The structure of the report was as follows:

- An outline of capsize issues, based on previous NSSWG work.
- An outline of risk assessment approaches.
- Background on Human Factors issues relevant to Human Reliability Analysis.
- A review of approaches to and steps involved in Human Reliability Analysis.
- Recommendations for steps to determine an approach to Human Reliability Analysis for Capsize risk, building on previous NSSWG work.

The recommendation of this report is that the NSSWG committee adopts a four-step 16- 24 month (depending on scheduling options) study to build on current NSSWG work and resources.

1. Extend the current MIL Systems capsize fault tree analysis into HF issues to select areas for application of the HRA approach.
2. Further investigate the costs and suitability of facilities and other resources (such as naval Subject Matter Experts) required for the HRA study.
3. Produce a detailed HRA study plan.
4. Conduct an HRA study in the identified area(s) of interest to provide risk estimates for a range of Human Reliability issues and to validate the HRA process in its application to capsize issues. Based on the outcome of this study, determine the utility of the HRA approach for NSSWG standards requirements and modify as required.

Depending on the scope and approach finally adopted for step 4, the rough estimated cost for this work is between CAN$140k and CAN$190k (i.e. US$15-20k / member).

104-05570/

Table of Contents

ABSTRACT I

EXECUTIVE SUMMARY II

TABLE OF CONTENTS III

LIST OF TABLES IV

LIST OF FIGURES IV

1. INTRODUCTION 1

1.1 GOALS 1
1.1.1 Global goal *1*
1.1.2 Project goal(s) *1*
1.2 REPORT STRUCTURE 1
1.3 ACRONYMS 1

2. OUTLINE OF CAPSIZE ISSUES 2

3. OUTLINE OF RISK 4

4. HUMAN RELIABILITY 12

4.1 HUMAN FACTORS IN SYSTEM DESIGN AND OPERATION 13
4.1.1 Human Factors and system life cycle *14*
4.2 HUMAN RELIABILITY ASSESSMENT (HRA) 15
4.2.1 Generic approach *15*
4.2.2 Outline of Some Key models *24*

5. RESOURCE REQUIREMENTS 31

6. DISCUSSION 35

7. RECOMMENDATIONS 40

9. REFERENCES 41

ANNEX A: PROJECT WORK TASKS A-1

ANNEX B: SUPPLEMENTARY INFORMATION B-1

List of Tables

TABLE 1: CONSEQUENCES: EXAMPLE SCALE FOR SUBJECTIVE ASSESSMENT 5
TABLE 2: LIKELIHOOD: EXAMPLE SCALE FOR SUBJECTIVE ASSESSMENT 6
TABLE 3: EXAMPLE RISK MATRIX 7
TABLE 4: PARTIAL HF HAZOP EXAMPLE FROM AIR TRAFFIC CONTROL 8
TABLE 5: EXAMPLE OF FUNCTIONAL FAILURE-BASED FMEA 9
TABLE 6: POTENTIAL TASK DESCRIPTION AND TECHNIQUES 18
TABLE 7: POTENTIAL ERROR IDENTIFICATION TECHNIQUES 20
TABLE 8: POTENTIAL REPRESENTATION TECHNIQUES 21
TABLE 9: POTENTIAL QUANTIFICATION TECHNIQUES 22
TABLE 10: POTENTIAL RISK REDUCTION TECHNIQUES 23
TABLE 11: GENERIC ERROR MODELING SYSTEM 29
TABLE 12: PLAN FOR HUMAN RELIABILITY ANALYSIS 39

List of Figures

FIGURE 1: THE RISK ASSESSMENT PROCESS 4
FIGURE 2: SIMPLE EVENT TREE FOR VESSEL CAPSIZING EVENTS 10
FIGURE 3: EXAMPLE OF PARTIAL FAULT TREE (ADAPTED FROM MIL SYSTEMS REPORT) 11
FIGURE 4: BASIC HF MODEL 14
FIGURE 5: HF INTERVENTION STRATEGIES FOR RISK MITIGATION 15
FIGURE 6: A GENERIC MODEL OF HUMAN RELIABILITY ANALYSIS (FROM KIRWAN 1994). 16
FIGURE 7: FAULT TREE SHOWING POTENTIAL AREAS FOR HUMAN RELIABILITY ANALYSIS (BASED ON MIL SYSTEMS REPORT) 17
FIGURE 8: SIMPLE DECISION ACTION DIAGRAM 19
FIGURE 9: TABULAR ANALYSIS OF ONE PART OF A BRIDGE WATCH-KEEPERS TASK. 19
FIGURE 10: RASMUSSEN'S SRK MODEL 25
FIGURE 11: RASMUSSEN'S DECISION LADDER 26
FIGURE 12: WICKENS' HUMAN INFORMATION PROCESSING MODEL 27
FIGURE 13: REASON'S BARRIER ALIGNMENT MODEL 29

1. Introduction

This report was prepared under the direction of DGMEPM DMSS 2-2 within PWGSC Contract No. W7711-017747/001/TOR (Call-Up 7747-14).

1.1 Goals

Global and Project goals are shown below.

1.1.1 Global goal

To determine a method to estimate impact of human reliability on risk of capsize.

1.1.2 Project goal(s)

To draft a strategic plan to:

- Review methods to identify and quantify the impact of human reliability on capsize probability.
- Establish the resources required (and facilities available).
- Recommend an appropriate approach for NSSWG to adopt.
- Conduct limited validation of the utility and feasibility of the recommended approach.

The Strategic plan to be presented to the June 2003 NSSWG meeting in Halifax.

1.2 Report structure

The report is structured as follows. After a brief outline of key concepts in Risk Assessment, Ship Stability, and Human Factors, subsequent sections will then deal in more detail with:

- methods available for assessment of the role of human reliability on risk of capsize
- general approaches to mitigation of risks due to human reliability,
- resources needed / available to carry out the methods / approaches identified,
- options for future work, estimated resource requirements, and associated trade-offs,
- recommendations for immediate work and a strategy and plan to carry out such work.

Separate Annexes contain Project Tasks and Literature search details.

1.3 Acronyms

DGMEPM	Director General Maritime Equipment Program Management	FTA	Fault Tree Analysis
PWGSC	Public Works & Government Services Canada	HRA	Human Reliability Analysis
SOW	Statement of Work	PSF	Performance Shaping Factor
NSSWG	Naval Ship Stability Standards Working Group	MicroSAINT	Network modelling software; basis for IPME
HF	Human Factors	SME	Subject Matter Expert
DMSS	Department of Maritime Ship Support	SRK	Skill, Rule and Knowledge (behaviour model)
DND	Department of National Defence	GEMS	Generic Error Modelling System
HAZOP	Hazard and Operability Study	IPME	Integrated Performance Modelling Environment
		ROM	Rough Order of Magnitude
		RCNC	Royal Corps of Naval Constructors
		OGWTG	Operational Guidance and Training Working Group
		USN	United States Navy

2. Outline of Capsize Issues

The purpose of this section is to outline the main issues associated with ship capsize and is based on earlier work by NSSWG and the MIL report "CF Ship Stability Risk Assessment" prepared for the Canadian DND in 2001.

On 17th December 1944, a fleet of over 80 American warships (destroyers, cruisers and aircraft carriers) in the Pacific received warning of an incoming typhoon. The ships' companies made the preparations they could but after an unequal struggle, three destroyers had capsized and sunk, several other ships were severely damaged, and nearly 800 lives had been lost.

After action reports record the professionalism, desperate measures and universal courage among the crews, many of which had begun their naval careers barely three years before, after 6th December 1941. The aftermath included research into ship design criteria that resulted in more stringent warship hull design standards for stability and capsize (Sarchin et al 1962). Those design standards have stood the test of time in that no warship has been known to be lost under similar conditions since.

However, ship by ship reports of the events during that typhoon contain clues to another class of causal factors that underwent only limited analysis at the time. Some ships of the same or similar class or design were lost while some were not. The decisions and the actions of commanders and crews before and during the event had a significant bearing on the outcomes.

Here is a small selection taken from the reports at the time. Before the storm, each commander considered the loading of his ship, in particular fuel and liquid ballast. Most commanders tried to load as much fuel and water as they could to add weight to their ship, lower its centre of gravity and make it more stable.

Not all had had the opportunity to do this fully. Some of those that could not fully load, distributed what the load they had to trim the ship in readiness for the likely direction of wind and waves in relation to the course they would be required to take. In other words, to place the weight towards the side of ship against which the pressure of wind and waves would come, thereby reducing the tendency to roll over. All the ships went through the standard procedure of preparing for heavy weather by securing heavy loads. Some commanders attempted to trim their ships by moving the crew to the windward side of the ship so that their weight would counteract the force of the wind and waves.

During the typhoon, different ships sustained different levels of damage or malfunction to key items of equipment such as the propulsion system, the steering gear, and fire fighting gear. Flooding took place in some, altering the stability characteristics of the ships, and hence their handling characteristics. Some had to contend, at the same time, with fires.

Many commanders and crews were experiencing that level of sea and wind conditions for the first time in particular the degree of rolling of the ship, and the impact of wind and wave on one side of the ship. Different commanders took different decisions about how to handle their ships. In particular, they took different decisions about when to diverge from the ordered speed and/or course of the fleet as a whole to save their own vessel. That is, when the risk of damage to or loss of the ship outweighed or rendered redundant the risk to the mission. In this, the influence of the navy culture, the perceived consequences of disobedience to orders, and the need for a clearly defensible reason for departing from those orders were probably factors in individual decisions to change course and speed to protect their ship.

In sum, differences in human decisions and actions, before and during the event, preparatory and reactive, had a major influence on the outcome. Admiral Nimitz in his letter to the US Navy after the event identified the difficult challenge facing each ship's commander: i.e. to balance the shades of gray and decide between safeguarding his ship and obeying orders to follow a certain course and speed, amid stressful, confusing and conflicting circumstances.

More recently, there has been increased interest in the role of human decisions and actions in major disasters, and their precursors, in order to be able to identify, predict and mitigate risk. Incidents have included nuclear power (Three Mile Island, Chernobyl,), chemical industry (Flixborough, Bhopal), oil platforms (Ocean Ranger, Piper Alpha), maritime tankers and ferries (Exxon Valdez, Herald of Free Enterprise), railway disasters, and numerous others.

In each case, human decisions and actions have played a key role. It has become almost conventional wisdom that 80% of accidents are the result of human actions, sometimes called human error.. However, while there has been acknowledgement of the significance of such human decisions and actions, there is also a tendency to either reject serious analysis and management as being just too complex to achieve or to adopt a "modify the worker" perspective. Sufficient risk mitigation can be achieved, it is assumed, through operator training (a "finger in the dyke" approach i.e. teach operators to recognize the signs and how to act); operator replacement (choose someone who can do better or automation) or, modification of motivation (through punishment or reward). Tempting as these approaches may seem they have met with very limited and largely temporary success.

Capsize itself may be regarded as a top level system failure. Capsize prevention may be subdivided into two major parts: ship design and subsequent operation. These two parts are not mutually exclusive since life cycle modifications to equipment and design may affect stability while operational procedures adopted with respect to ship loading and handling in relation to sea conditions will interact with the design. All of these aspects will be affected by regulations, guidelines, and training of designers and ship operators.

Two major technical factors related to the probability of capsize are Buoyancy and Stability. Both these factors will fluctuate as a result of interaction with other influences such as design (original and upgrades), loading (fuel, people, cargo), and ship handling (speed, heading, manoeuvring). Other influences include sea state (wave and wind direction and forces) and the training of those responsible for managing any of the above under normal circumstances and in response to malfunction or damage. (For this report, only intact ship issues are considered.)

- Any of the above may affect *buoyancy* via water accumulation, or excessive weight.
- Any of the above may affect *stability* via light ship weight growth, ship loading of all forms of cargo, free surface liquids, wave synchronicity, size and direction.

Depending on the availability of data on any of the above, appropriate formula allow predictions about both Buoyancy and Stability in relation to Capsize Probability (e.g. McTaggart et al 2002).

Sources of relevant data include experiments and tests conducted with real ships and with models in various forms of simulators; incident and accident investigations; empirical data from sensors on ships, seaways; and anecdotal reports from observers.

3. Outline of Risk

This section provides a brief outline of risk assessment and serves as a basis for much of the remainder of the report.

In everyday terms, *risk* is seen as inherent in all activities and can be described as the *probability* of an adverse consequence or *hazard*. A *hazard* is a source of harm or failure. Further analysis of risk requires identification of *hazards*, their *frequency* of occurrence, and the *severity* of the consequence(s). Probabilities and consequences may be categorised in different ways but are commonly expressed as a matrix such as that illustrated below.

Acceptability is another key term since risk is unavoidable and cannot, in practice, be eliminated. *Risk management* requires some trade off between the methods of risk mitigation adopted, the cost of their implementation (including the denial of limited resources to management of other risks) and the likely benefit(s). *Acceptability* is not absolute. Risks acceptable for one group of people (employees) may not be for another (the public). Risks acceptable under one set of circumstances (war) may not be for another (peace). Different consequences of the same event have different levels of acceptability (damage to property, injury or death). Thus, risk assessment cannot be conducted independently of societal values, resources and circumstances.

In outline, the Risk Assessment process is as follows.

Figure 1: The Risk Assessment Process

Risk evaluation may be qualitative or quantitative – although never wholly the latter.

- Qualitative approaches are commonly based on the judgement of experts – i.e. those sufficiently familiar with the system in question and its operation to be able to estimate probabilities, consequences, risk management options and their costs. Acceptability may be judged by those affected by or responsible for the perceived outcomes: e.g. individuals, managers, and politicians.
- Quantitative approaches depend on access to objective data about event frequencies and consequences and theoretical valid formulae relating these. In practice, comprehensive and relevant data bases are difficult to compile and developing valid algorithms for complex relationships is extremely challenging.

Within this broad distinction, several evaluation methods exist.

- **Risk Matrix**

  This is the simplest form of qualitative risk assessment used for high level, rough estimates. Analysis is based on agreed potential mishap scenarios using a structured hazard analysis technique. Each scenario is then assigned a perceived level of acceptability by the analysis team using a Risk Matrix.

  The Risk Matrix has two components: Consequences and Likelihood. Consequences might be described as in Table 1.

		Consequence		
Rank	**Description**	**Human**	**Asset**	**Financial**
10	Catastrophic	Multiple Deaths >10% complement		>$500 million
9.5	Disastrous	Multiple Deaths <10% complement >1	Total loss of vessel	<$500 million >$50 million
8	Critical	Single Death and / or Multiple Severe Injuries	Major damage to vessel. Temporary abandonment. Mission aborted	<$50 million >$5 million
6.5	Marginal	1-2 severe injuries and/or multiple minor injuries resulting in hospitalisation but < 25 days lost work.	Significant damage to vessel. Mission degraded.	<$5 million >$0.5 million
4.5	Minor	At most, one minor injury leading to in single lost work day, after day of injury	Minor damage to vessel. Mission unaffected	<$0.5 million >$50 thousand
3	Negligible	Minor injury. No lost work day.	Negligible damage to vessel	<$50 thousand

Table 1: Consequences: Example Scale for Subjective Assessment
(From MIL Systems Report)

Likelihood or probability of occurrence might be described as in Table 2.

Probability	Rank	Description
>0.1	10	Greater than 10% chance of occurring each year. Will occur more than once in every ten ships each year
0.1	9	10% chance of occurring each year. Will occur once in every ten ships each year.
0.01	8	Expected to occur once in 100 ships each year or once in every ten ships every ten years.
0.001	7	Expected to occur once in 100 ships every 10 years or once in every 1000 ships every year.
0.0001	6	Expected to occur once in 1000 ships every 10 years or once in every 10,000 ships every year.
0.00001	5	Expected to occur once in 1000 ships every 100 years or once in every 100,000 ships every year.
0.000001	4	Expected to occur once in 10,000 ships every 100 years or once in every 100,000 ships every 10 years or once in every 1,000,000 ships every year
0.0000001	3	Expected to occur once in 100,000 ships every 100 years or once in every 1,000,000 ships 10 years or once in every 10,000,000 ships every year

Table 2: Likelihood: Example Scale for Subjective Assessment
(From MIL Systems Report).

Frequency and consequence categories can be developed qualitatively or quantitatively.

- *Qualitative* schemes (i.e. low, medium, or high) are descriptive, based on estimates generated by experts familiar with the system and circumstances. These schemes typically use criteria and examples of each category for consistent event classification. Multiple consequence classification criteria may be required to address safety, environmental, operability and other types of consequences.
- *Quantitative* schemes are based on objective occurrence data, where reliable data exists. This is a particular challenge for human reliability data.

Once assignment of consequences and likelihoods is complete, a risk matrix can be set up (see Table 3 below) for risk acceptance decisions for each identified scenario. Each cell in the matrix corresponds to a specific combination of likelihood and consequence and can be assigned a priority number or some other risk descriptor.

Frequency Rating			Consequence Rating					
			10	9.5	8	6.5	4.5	3
Probability	Rank	Descnption	Catast rophic	Disas trous	Crit ical	Marg inal	Minor	Neglig -ible
>0.1	10	Greater than 10% chance of occurring each year. Will occur more than once in every ten ships each year	100	95	80	65	45	30
0.1	9	10% chance of occurring each year. Will occur once in every ten ships each year.	90	86	72	59	41	27
0.01	8	Expected to occur once in 100 ships each year or once in every ten ships every ten years.	80	76	64	52	36	24
0.001	7	Expected to occur once in 100 ships every 10 years or once in every 1000 ships every year.	70	67	56	46	32	21
0.0001	6	Expected to occur once in 1000 ships every 10 years or once in every 10,000 ships every year.	60	57	48	39	27	18
0.00001	5	Expected to occur once in 1000 ships every 100 years or once in every 100,000 ships every year.	50	48	40	33	23	15
0.000001	4	Expected to occur once in 10,000 ships every 100 years or once in every 100,000 ships every 10 years or once in every 1,000,000 ships every year	40	38	32	26	18	12
0.0000001	3	Expected to occur once in 100,000 ships every 100 years or once in every 1,000,000 ships 10 years or once in every 10,000,000 ships every year	30	29	24	20	14	9

Table 3: Example Risk Matrix
(From MIL Systems Report)

- **Hazard and Operability Analysis**

The HAZOP analysis technique uses special *guidewords* to prompt an experienced group of individuals to identify potential hazards or operability concerns relating to pieces of equipment or systems. *Guidewords* describe potential deviations from design intent and are created by applying a pre-defined set of adjectives (i.e. high, low, no, etc.) to a pre-defined set of process parameters (flow, pressure, composition, etc.).

The group brainstorms potential consequences of these deviations and if a legitimate concern is identified, determine if appropriate safeguards are in place to help prevent the deviation from occurring.

The purpose of a HAZOP is to identify deviations away from the intended functioning of the system. Therefore, for instance, if the guide word '*no*' was applied to the selection of a 'menu' in an Air Traffic Control software system, a deviation such as '*no heading entered into system*' would be identified. In turn, for each deviation, the group would go on to identify the consequences of the error on the system, indications that the error occurred, system defences and ways in which such an error would be recovered or reduced.

This type of analysis is generally used on a system level to generate qualitative results, although some simple quantification is possible. The primary use of the HAZOP methodology has been to identify safety hazards and operability problems of continuous

process systems. Many aspects of ship operation can be viewed as a continuos process system. A partial HAZOP example is shown in Table 4 below.

Function	Cause	Consequence	Indication	System Defences	Human Recovery	Recommendation
Highlight Object	Another item preventing access to target	Difficulty in hooking target aircraft	No highlighting of target	None	Drag blocking object out of way; Strategic management of screen items	Design objects to roll around each other; Height filtering; Flip system to move between object on top and the one beneath; Highlight background tracks
	Clustering results in different aircraft being highlighted instead of target	Instruction may be given to wrong aircraft on the system	As Above	Implicit focus is colour coded to indicate direction of travel; Call sign is displayed on all menus	As Above	As Above

Table 4: Partial HF HAZOP example from Air Traffic Control

- **Failure Mode and Effects Analysis (FMEA)**

FMEA is an inductive reasoning approach best suited for reviews of physical subsystem components of an overall system. Although applicable to any well-defined system, the primary use has been to review mechanical and electrical systems (e.g. fire suppression systems, vessel steering/propulsion systems).

The FMEA technique considers (1) how the failure mode of each sub-system component can result in system performance problems and (2) whether appropriate safeguards against such problems are in place. The technique can be used to define and optimise planned maintenance for equipment because the method focuses directly on individual equipment failure modes.

FMEA generates qualitative descriptions of potential performance problems (failure modes, root causes, effects and safeguards) and can be expanded to include quantitative failure frequency and/or consequence estimates.

The general format for FMEA is shown below.

unctiona Failure	Loss Scenario (Effect)	% teportabl Marine Events	Dominant Causes	Applicable Inspection Activity	ıspectio Effort	Criteria	Change in Risk
Function: Providing Start Air for Engines							
No or insufficient volume of start air provided to engines	No engine start, which can lead to loss of propulsion and a disabled vessel Could possibly lead to a grounding, collision, etc.	~25%	Condensation in bottles (62%)	Blow down bottles during inspection	<10 minutes	Do not have to do on variable pitch propellers	Current practice (high negative impact if not performed)
				'erify that regular low downs are cheduled and ccurring (by scord review)	5 minutes	iee above	ossibly high ositive impact
				Communicate importance of blow downs to crew	<5 minutes	See above	Current practice (high negative impact if not performed)
			Disabled compressors (multiple compressors) (5%)	Operation verification (measure discharge pressure)	<10 minutes	See above	Current practice (high negative impact if not performed)
				Visual inspection for leaks, gauges functioning, obvious defects, etc.	<5 minutes	See above	Current practice (high negative impact if not performed)
				Communication with pilots about known problems during transit	<5 minutes	See above	Current practice (high negative impact if not performed)

Table 5: Example of Functional Failure-based FMEA
(☐ = high impact item)

- **Event Tree Analysis**

Event tree analysis uses a decision tree format to model possible outcomes of an initiating event. This type of analysis can provide (1) qualitative descriptions of potential problems (combinations of events producing various types of problems from initiating events) and (2) quantitative estimates of event frequencies or likelihoods, which assist in demonstrating the relative importance of various failure sequences.

Event tree analysis may be used to analyse almost any sequence of events, but is most effectively used to address possible outcomes of initiating events for which multiple safeguards are in line as protective features.

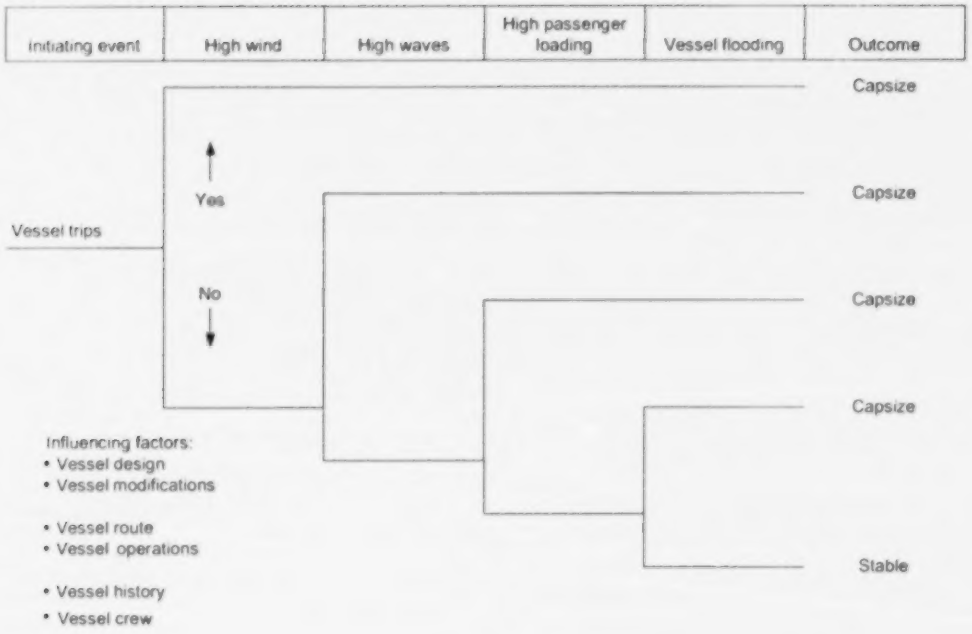


Figure 2: Simple Event Tree for Vessel Capsizing Events

- **Fault Tree Analysis**

Fault Tree Analysis (FTA) is a deductive analysis that uses Boolean logic to model how relationships among equipment failures, human errors and external events can combine to cause specific mishaps of interest. Similar to event tree analysis, this type of analysis can provide (1) qualitative descriptions of potential problems (combinations of events causing specific problems of interest) and (2) quantitative estimates of failure frequencies/likelihoods and the relative importance of various failure sequences/contributing events.

This technique has many applications, but is most effective for analysing system failures caused by relatively complex combinations of events. See below for an example.

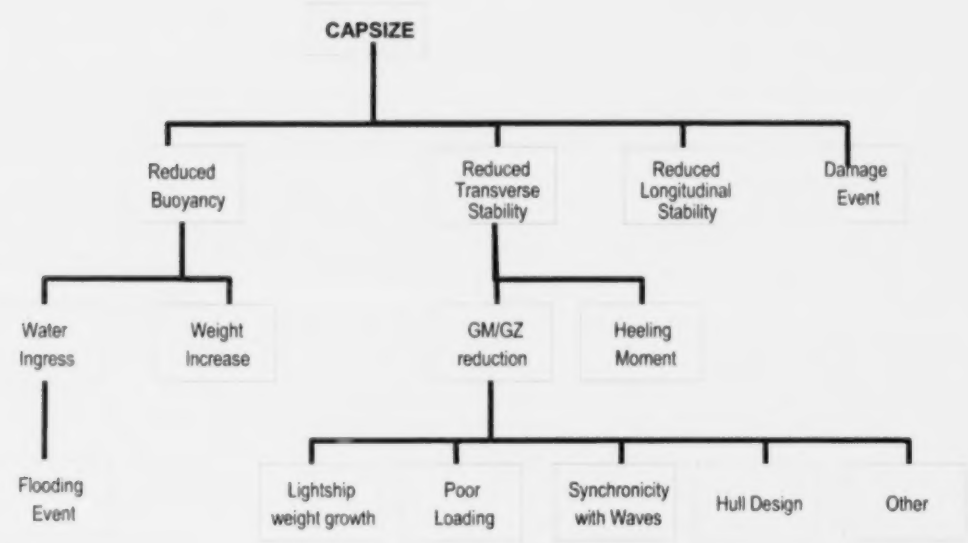


Figure 3: Example of partial Fault Tree
(Adapted from MIL Systems Report)

Any of the methods outlined above can be used to investigate Human Factors issues. These issues may to identify hazards, assess risks and determine the effectiveness of potential risk mitigation measures associated with the interface of human operator(s) with hardware / software components of any system. Hazard identification guide words have been developed to prompt a review team to consider human factors design issues.

4. Human Reliability

This section will set the concept of Human Reliability within a broad Human Factors (HF) model and draw out elements of HF relevant to risk assessment and mitigation of ship capsize.

The Human Reliability Assessment (HRA) process has three components: hazard identification, risk quantification, and mitigation. A widely used term is "Human Error" i.e. human behaviour that leads to a hazardous condition or system failure. Some question the use of the term "Human Error" since it carries implications of blame. A satisfactory substitute for the term "Human Error" has never been generally accepted (although 'Human Variability' has been used), but the implications of "*blame*" are not useful for the purposes of risk analysis and investigation.

Perceptions of blame associated with the term "human error" can lead to a chilling effect when discussing particular incidents with those involved. It can also lead to truncation of analysis at the level of operators involved or their first line supervisors rather than the functional system as whole, with operators considered as part of the system. Such truncation can, in turn, lead to the inappropriate assumption that the only or the best HF risk mitigation strategy is to change the operator(s) through training, replacement, or discipline, or to substitute human involvement with some form of automation or mechanisation.

While risk mitigation strategies involving substitution or changing the operator(s) may be viable in some instances, a broader approach to risk mitigation is to first identify and then modify those factors that influence behavioural outcomes in the first place. Such factors include Performance Shaping Factors (PSFs) such as fatigue, cognitive complexity, workload, interface design, organisational and job design and corporate culture. System design and the context of operation in turn, influence these factors.

Human action or inaction in complex and unforgiving systems can lead, directly or indirectly, to reduced performance, or failure of all or part of the system. Such actions or in-actions may achieve their influence in isolation or as a result of some chain of events. The actions (or in-actions) of the operator can also lead to reduced capability in the overall system.

Consider a simple example. Each day ten thousand vehicles negotiate a busy road junction. Each day one hundred drivers may perform a given behaviour (such as checking in only one direction) that increases the risk. On most occasions, there will no ill effect. The factors that influence the behaviour will vary: a distracting passenger, a belief that there is no need to check. There will have to be a second behaviour instance, say a child running from a parent from a behind a parked vehicle to create the combination of events that lead to collision. The severity of the outcome will also vary from a slow down in traffic to death, according to the combination of circumstances, including the degree of attention shown by other drivers. The multiple permutations and combinations underline the challenge of analysing the impact of human behaviour in such a situation and to recommending risk mitigation strategies.

In spite of the complexity in describing the full gestation of an incident, Human Error Probability has been defined simply as:

$$\frac{\textit{the number of errors that occur}}{\textit{the number of opportunities for error}}$$

This definition invites a data base approach and fits within probabilistic risk assessment approaches. However, in many instances, human error does not have any appreciable effect because of other safeguards or because the required combination of factors did not occur. This

means that in most cases the reported number of errors is probably a fraction of the actual number that occurs.

Early approaches to HRA sought to establish failure rates for operators in much the same way this might be done for failure of a mechanical component. By and large, this approach has been considered unsatisfactory (Kirwan et al, 1994), largely because humans are more complex, subject to a greater range of influences and, consequently, are not so predictable in their reactions as hardware. Also even simple human / human interactions add a further dimension of complexity.

As a consequence, estimates of human behaviour for risk assessments tend to rely on systematic and exhaustive qualitative analyses based on expert opinions, rather than quantitative analyses that use data such as reported error rates and experimentally-derived figures that reflect the influence of PSFs. Reported error rates are not available. Investigating the influence of PSFs requires too great an investment, and is too subject to complex interactions.

Rather, the general approach is to provide a carefully assembled multidisciplinary team of HF specialists and experienced operators with a detailed description of human behaviour for the task(s) of interest. This team considers how operator performance can vary, and whether the consequences of the variability are acceptable. If the variability is not acceptable, then a risk mitigation strategy is devised, implemented and the outcome monitored. There will nearly always be a choice of mitigation strategies (see Figure 3 in the next section), with trade-offs to be considered.

4.1 Human Factors in system design and operation

This section outlines of the interaction of human operators within systems and provides a basic model of Human Factors (HF).

When a complex system, such as a ship, is designed, the design has to support a range of functions. Based on trade-offs among a number of aspects such as budget, purpose of the design, technologies available, personnel costs, complexity (etc) assignment of any given function will be divided in some way between human operators, hardware and software.

Whatever the division, at some level, human operators will serve a control function with some interface device (or combination of devices) to provide them with the information needed to make their decisions and the means of control to implement the decisions. Teams may further subdivide functions between them. The trend is away from using human operators to fulfil physical functions such as lifting and carrying, and towards information processing functions such as fusing and interpreting data and information and making decisions.

To perform the system function assigned to them, the operator must use the facilities provided to take in information about the system and its environment through their different senses, interpret that information based on training and experience, and make a decision to act (or not) upon the system as appropriate. Depending on the level of complexity and predictability of the situation and the training and experience of the individual, behaviours may be routine and based on procedural rules or ingrained skills, or may require more complex and creative information seeking and analysis.

The choice or manner of the interaction will vary with the characteristics of each person, the physical qualities of the environment in which they work; the training system through which they have come; and organisational factors such as hours of work; and attitudes shaped by the culture of the organisation. It is likely that operators of a given part of the system will share a particular profile (age, socio-economic group, training, experience, level of fitness, attitudes, etc) and this profile will make their reactions more predictable.

This overall picture is illustrated below.

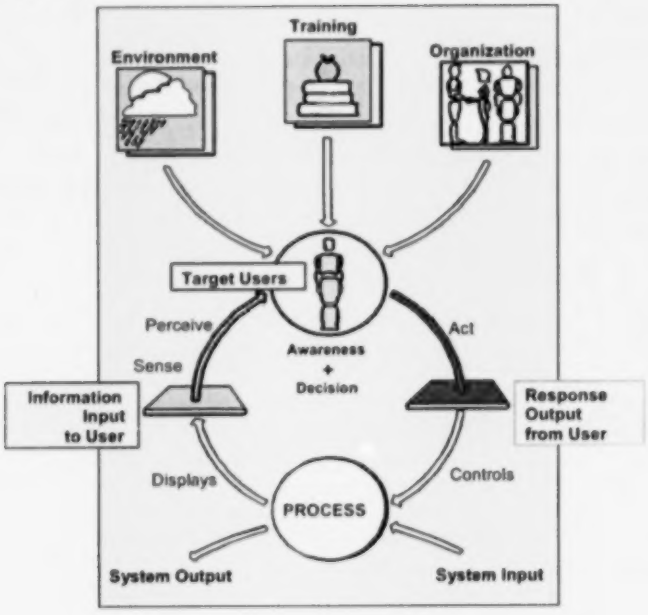


Figure 4: Basic HF Model

For a given class of system, such as ships, and for a given function, such as steering the ship, the technology provided and the job itself may differ significantly from system to system (ship to ship). Some ships may be steered from the bridge where the helmsman can look out over his/her surroundings. In others, the helmsman may work in a separate compartment in response to verbal directions without being able to see where the ship is going. In smaller craft, the helmsman may also be the bridge watch-keeper, or even the captain. The helmsman may be responsible for controlling the propulsion system, or not at all.

Such differences must be understood through the process of task description and analysis, for which there are several different approaches. These are outlined later in the section on Human Reliability Assessment and are used to describe the characteristics of the system, representative user profiles, performance shaping factors, and behavioral and cognitive activities and consequences, including errors.

All HF work assumes that the causes and consequences of human behaviour are sufficiently generic for HF work in one domain to be transposed to another (e.g. between industrial process control and piloting a ship), with identification of and allowance made for critical differences between domains and tasks.

4.1.1 Human Factors and system life cycle

Even though the current NSSWG focus is on risk identification and assessment, it is likely that human factors will be identified as a serious risk factor in one way or another. If so, risk mitigation will become an issue at some point in the system life-cycle with respect to design or operation. Consequently, this section is included in the report as background.

To optimise the relationship between human operators and the work they perform, there are three possible categories of intervention strategy. (In the context of this report, these can be seen as synonymous with risk mitigation strategies.) These strategies include:

- User friendly design that fit users' sensory, perceptual, cognitive and physical characteristics.
- Provision of appropriate training support (embedded or otherwise) to provide the user the requisite knowledge and skills in conjunction appropriate recruiting techniques to establish the appropriate profile of qualifications and abilities and to screen candidates for that profile.
- Design of jobs, teams and organisational culture to ensure the most effective motivational and social environment for the type of work involved.

These three aspects are not mutually exclusive, and will arrive at some balance in any system. The goal of Human Factors is to identify the issues involved and select the most appropriate balance, preferably pro-actively as the system is designed, developed, and staffed, rather than reactively as problems emerge during the operational life cycle. Shortcomings in any of the above can lead to under performance of individuals and hence the system as a whole.

Figure 5: HF intervention Strategies for Risk Mitigation

4.2 Human Reliability Assessment (HRA)

This section outlines a generic approach to Human Reliability Assessment and key models and concepts. The goal of this section is to provide the reader with a broad understanding of HRA options and their pros and cons.

4.2.1 Generic approach

The approach outlined below shows a generic approach in identification, quantification and mitigation of the human impact on risk. In the remainder of this section, key models relevant to the application of this model, and each step is discussed in greater detail, and related to ship capsize issues.

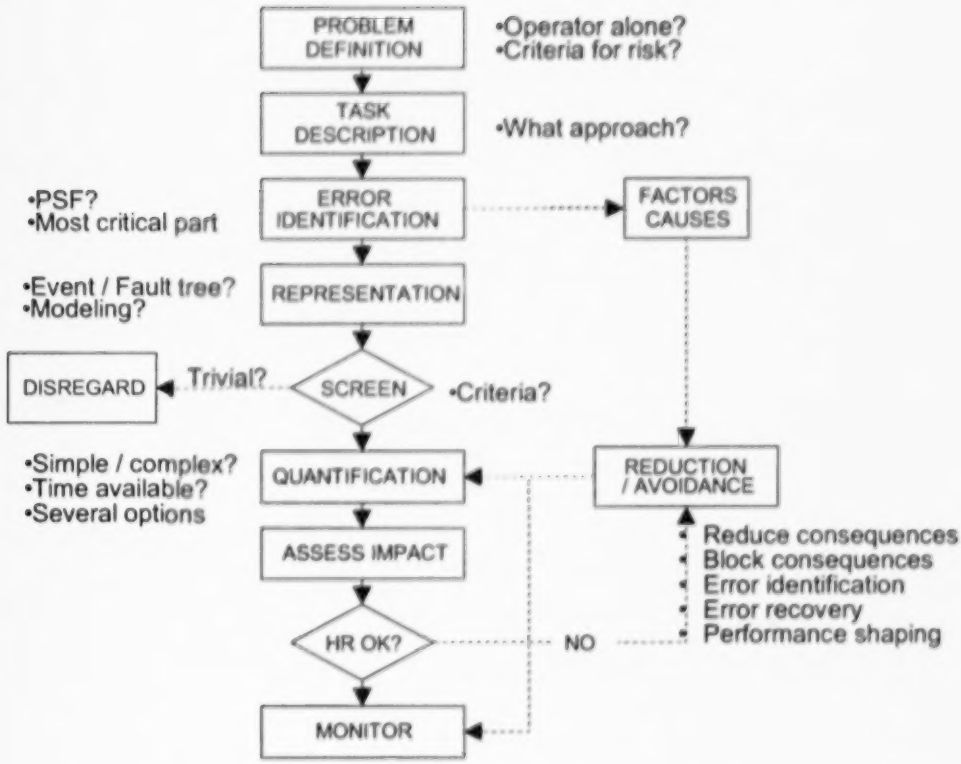


Figure 6: A Generic model of Human Reliability Analysis
(from Kirwan 1994).

4.2.1.1 Problem definition

Define Problem	Describe Task	Identify Errors	Represent Analysis	Screen & Quantify	Assess Impact	Reduce Risk	Monitor Outcome

During this phase, the scope of the HRA will be determined. The relationship with other Probabilistic Safety Assessments, the types of errors to be considered, whether a quantified estimate of reliability is required, how that estimate is calculated, etc. need to be determined at this stage. The scope may change slightly during the HRA, but the single most important focus will continue to be "is it safe?"

In the context of ship stability, previous work (MIL Systems, 2001) has produced a fault tree analysis of the risk to ship stability for intact ships, and ships with 1, 2 or 3 compartments flooded. In the intact ship example, there are at least 22 separate faults that can be attributed at least to some degree to human activities during or before the incident (see below). Each of these could become the subject of its own task description and subsequent risk analysis. The MIL Systems fault tree would allow Human Factors issues of interest to be identified and estimates of the scope of the work to be undertaken.

Each of the areas in the partial fault tree shown below have the potential to be further broken down in terms of the Human Factors issues outlined above, and the contribution to risk assessed. For example, poor loading might be influenced by error prone interface design, organizational culture, division of responsibilities between different departments in the ship, the impact of factors such as fatigue or sea-sickness on attention and decision making, training, or motivation.

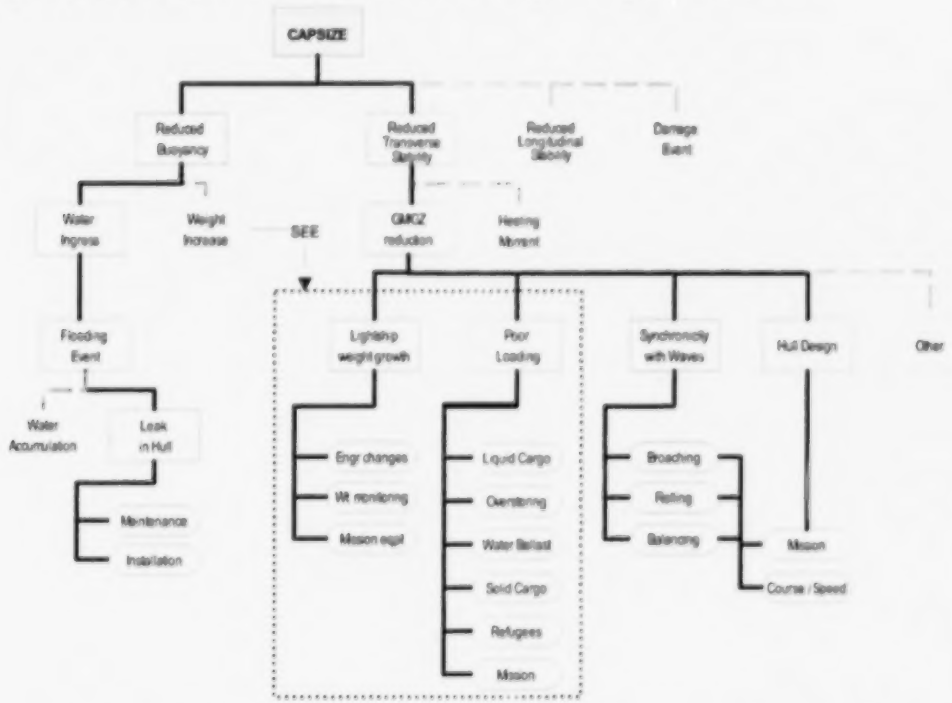
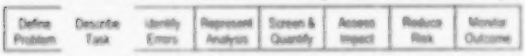


Figure 7: Fault tree showing potential areas for Human Reliability Analysis
(Based on MIL Systems Report)

4.2.1.2 Task Description and Analysis



Task description defines in detail the roles of the operators within the system (much like a blue print) and is an integral part of the HRA process. The task description will become the basis of experts' judgements and calculations of overall human reliability. In some techniques, the description and the analysis are performed in parallel.

There are a variety of different task description techniques, each suitable for different domains or analysis goals (see Table 6 below). The application of task description is fairly straightforward but relies heavily on opportunities to observe and / or interview operators about their task behaviour, and the level of system information provided to the analyst. Depending on the scope and depth of the analysis, this stage can require a significant investment of effort. For example, computer simulation methods such as Micro-Saint can yield comprehensive models but time consuming to prepare. However, once compiled, these models can be used to estimate baseline probabilities, manipulated to compare different situations, eventually, to compare risk mitigation strategies. Thus a generic task model of bridge watch-keeping activities could subsequently be customized for different classes of ship or bridge layout and to assess the likely consequences of different bridge decision support options.

Technique	Focus	Examples
Task-data-collection approaches	Human-system interactions.	Observation, interview, documentation review, verbal protocol, critical incident technique, walk/talk through
Task-description approaches	Providing a structure for information collected so that the information can be used more easily.	Flowcharts, operational sequence diagrams, hierarchical task analysis, link analysis, decision-action diagrams, tabular task analysis, timeline analysis
Task-modeling methods	Compiling data on human involvement to create a more dynamic model of what happens during execution of a task.	Computer simulation Network modeling
Task-requirements-evaluation techniques	Assess the adequacy of facilities available to the operator for supporting execution of the task.	Checklists, surveys
Human reliability Assessment	System performance evaluation, usually from a safety perspective.	HAZOP, Event Trees, Fault Trees

Table 6: Potential Task Description and Techniques

An example of a common flow chart approach, the decision action diagram, is shown below. Such diagrams are readily understood by Subject Matter Experts (SMEs) gathered to analyze consequences and probabilities of different steps in a task, and also form the basis of more sophisticated approaches such as computer simulation models.

The level of break down depends on the detail required. Elements in the simple example below would be broken down further. Decision Action Diagrams can be arranged in Swim Lanes to show team decision making, with a different lane for each person in the team, and showing exchange of

information and inter-dependence of decision making among team members. An example might be the division of responsibility for different factors affecting ship stability issues shown in the fault tree among different departments of the ship (such as ship loading and ship handling), or among different members of a bridge watch-keeping team.

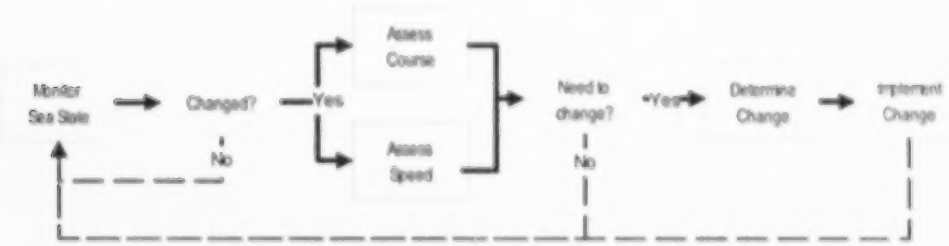


Figure 8: Simple Decision Action Diagram

Another task description format is Tabular Task Analysis. This sets out the initiating cues and sources of information and feed back provided by the system for the steps in any given task. This format is illustrated below in Figure 9.

Step or task	Initiating event or cues	Information required	Information source	Action	Feedback on outcome
Watch- keeper Assess Course	Sea condition Wind strength Ship traffic Route turning point Navigation hazard Change in mission Ship Malfunction etc	Surrounding Traffic Weather prediction Condition of ship Local hazards Mission goal(s) etc	Chart Visual Radio traffic Chart Radar Lookout Captain	Helm order	Helm indicator Radar picture Ship motion Visual cues Radio traffic Lookout etc

Figure 9: Tabular Analysis of one part of a Bridge Watch-keepers task.

4.2.1.3 Error Identification

Define Problem	Describe Task	Identify Errors	Represent Analysis	Screen & Quantify	Assess Impact	Reduce Risk	Monitor Outcome

Identification of errors is the most difficult part of a HRA. However, accident experience has shown that human errors, in many situations, occur in a limited number of forms, some of which are fairly predictable. There are a number of techniques for identifying errors, and these must be chosen carefully to ensure they adequately describe the factors surrounding the error (see Table 7 below based on Kirwan 1994). It is important that a human error identification process is comprehensive, because otherwise errors will not appear in the HRA and an inaccurate perception of reliability will result.

Technique	Basis	Method	Strengths	Weakness
1. Risk Matrix	Scenario	Expert judgement	Relatively low effort. Quick	Very High Level.
2. HAZOP HAZard & OPerability studies	Taxonomic	Task analysis, panel of experts' judgement based on guide words.	Early design stage Identifies errors in system.	Resource-intensive, need good group facilitator & strong HF representative.
3. THERP: Technique for Human Error Rate Prediction	Taxonomic (Berliner, Swain & Guttman)	Task analysis, expert judgement of error paths using taxonomy.	Straightforward & simple to use, can model all errors that can affect a system.	Lack of structure and inter-rater reliability. Excludes psychological mechanisms.
4. SRK Analysis (Skill-, Rule & Knowledge-)	Model (Rasmussen)	Analyse past incidents according to SRK model.	Considers psychological mechanisms, easy-to-follow flow chart.	Not predictive, can be resource intensive.
5. GEMS Generic Error Modelling System	Taxonomic	Hierarchical breakdown of errors to determine psychological error mechanisms.	Considers psychological mechanisms, includes biases, more comprehensive than SRK.	Guidance on choosing underlying errors is limited
6. SHERPA Systematic Human Error Reduction & Prediction Approach	Model (SRK & GEMS) & taxonomic.	Computerised question-answer routine (based on flowcharting approach) based on previous task analysis.	Considers psychological mechanisms, determines recoverability (immediate, later, not at all) of errors, links to error reduction measures, resolves errors to fine level of detail.	Unreliable, jargon ridden.
7. HRMS Human Reliability Management System	Model & taxonomic	Computerised modules for task analysis, human error identification.	Comprehensive & rigorous, provides documentation on analysis, confidence in findings.	Requires high degree of analyst expertise, resource intensive.
8. PHECA Potential Human Error & Cause Analysis	Taxonomic	See HAZOP.	See HAZOP.	See HAZOP.
9. TRACEr/HERA Technique for Retrospective Analysis of Cognitive Errors / Human Error Retrospective Analysis	Model & taxonomic	Flowcharting approach to characterise & identify possible errors.	Comprehensive, based on experience of all other techniques, easy to use, covers PSFs, EEMs, IEMs & cognitive domain.	Reliant on skill & familiarity of analyst (especially for predictive applications).

Table 7: Potential Error Identification Techniques

4.2.1.4 Representation

Define Problem	Describe Task	Identify Errors	Represent Analysis	Screen & Quantify	Assess Impact	Reduce Risk	Monitor Outcome

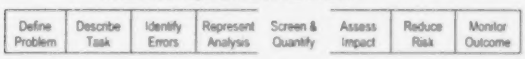
Once identified, human errors must be represented so that the probabilities and consequences of each individual error can be ascertained and the combined risk probabilities of all failure combinations (hardware, software, human and environmental) summed to show the total level of risk in a system. There are a number of different representation techniques, including fault and event tress and simulation techniques (see Table 8 below). Any representation technique should model dependencies between different identified human errors so that errors are not treated independently thus leading to artificially low calculated levels of risk.

If a large number of errors have been identified, it may be advisable to screen the errors before representing them. This process assigns each error a pessimistic probability and evaluates the total system risk. If any given error does not to strongly diminish system reliability, then it is excluded from further detailed analysis.

Technique	Approach	Analysis	Strengths	Weaknesses
Fault Tree	Begin with undesirable event and work backward to determine what events must occur in order to trigger the undesirable event. Events can occur singly (OR gate) or in combination (AND gate); can use frequencies or probabilities to calculate.	Probabilities for OR gates are added together; probabilities for AND gates are multiplied together; a probability multipled by a probability is a probability, a probability multiplied by a frequency becomes a frequency.	If many outcomes, fault trees may be more manageable, wholly accepted in risk assessment community.	Less good for tasks where one step depends upon the previous step.
Event Tree	Begin with an initiating event and then develop a logical set of outcomes; generally use AND/OR gates.	Multiply all probabilities for single branch to calculate probability of an outcome; calculations can be checked, because probability of all outcomes should be '1'.	Better for closely-couple tasks, time dependent tasks, wholly accepted in risk assessment community.	Difficult to create a comprehensive event tree if there are many possible outcomes.
Simulation	Conduct a task analysis and enter the task data into a simulation application (e.g. SAINT, IPME).	The simulation will run through the task in accordance with the rules set by the analyst, and in response to the initiating events entered by the analyst.	Can run through many episodes of a task, thus providing data on infrequent errors, can be modified to compare outcomes.	Resource intensive, some questions about validity of outputs.

Table 8: Potential Representation Techniques

4.2.1.5 Quantification

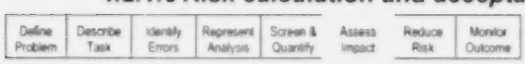


There are a number of validated tools available for human error quantification. These include expert-judgement techniques such as paired comparisons and absolute probability judgement, computer modelling and simulation, and a variety of computational databases (see Table 9 below). These approaches must be selected according to their maturity, validity and reliability within the chosen context (i.e. ship stability). In practice, this stage can be where the most effort is expended in HRA, but without this stage estimates of human reliability would not be possible. The options tabulated below require further investigation in terms of their suitability for HRA in the ship capsize context. Those relying heavily on extensive database material are likely to be less suitable, since such data is unlikely to be available (although some attempts to compile human reliability databases have been made, e.g. Computerised Operator Reliability and Error Database (CORE-DATA); Gibson, 1998). Mathematical approaches to estimating the likelihood of failure in systems that have never experienced a failure are not valid if used to determine human reliability. This is largely due to the variability in conditions surrounding human performance (i.e. more or less fatigued, more or less distracted, etc.). This supports an argument in favour of expert-judgement techniques.

Technique	Approach
. **APJ** Absolute Probability Judgement	Group of experts discuss each error before deciding upon a probability of occurrence.
. **Paired Comparisons**	Present all possible pairs of errors and for each pair an expert decides which one is more likely. To work, the probabilities of at least two errors must be known.
. **HEART** Human Error Assessment and Reduction Technique	Once a task is classified, the analyst must then choose relevant error probabilities from the database (part of the application). The application will multiply probabilities to calculate overall error probability.
. **THERP** Technique for Human Error Rate Prediction	Similar to HEART, but also incorporates PSF effects, etc.
. **SLIM-MAUD** Success Likelihood Index Method using Multi-Attribute Utility Decomposition	Computerised technique uses both a paired comparisons approach and a database of experimentally-derived data to calculate probabilities of errors.
. **STAHR** SocioTechnical Approach to Human Reliability assessment	Technique used to model difficult PSFs such as safety culture and management. Experts define how these PSFs influence error, including assigning probabilities.
. **HCR** Human Cognitive Reliability	Several variants, that focus on time as the primary PSF. Questions about its validity arising from simulation trials. Large amounts of development funding in the US.
. **ASEP** Accident Sequence Evaluation Programme	A short version of THERP that uses conservative values for screening. It is quicker than THERP and computerised, and can be used to screen errors in a larger THERP effort.
. **Micro- SAINT** Systems Analysis of Integrated Networks of Tasks	PC based simulation based on task analysis. Uses a Monte Carlo simulation to model the operator, thereby allowing a network of tasks to be 'run' dynamically. Task analysis must be comprehensive, but can provide data about infrequently occuring errors. An extension under development for DND called IPME (Integrated Performance Modelling Environment) allows modelling of environmental factors and individual differences.
0. **MAPPS** Maintenance Personnel Performance Simulation	A computerized, stochastic, task-oriented model of human performance similar to SAINT. Includes consideration of PSFs but focuses on maintenance workers.
1. **HRMS** Human Reliability Management System	Fully computerised system based on actual data and including consideration of PSFs and allowing the analyst to modify values. Requires a significant amount of training
2. **JHEDI** Justification of Human Error Data Information	Developed to provide a faster screening technique than its 'parent' (HRMS). Database is more conservative than HRMS and is less resource intensive. Application of the technique requires little training.

Table 9: Potential Quantification Techniques

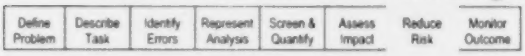
4.2.1.6 Risk calculation and acceptance



Having collected the data required to calculate human reliability (i.e. representation and quantification of errors) the overall level of system risk can be determined. From this calculation it can be decided if the system is acceptably safe and, if not, what the main approaches might be to reduce risk to an acceptable level i.e. risk mitigation strategies.

It may be the case that human error is the main factor in undesirably high risk levels and cannot be reduced without removing the human element. The HRA team need to establish exactly what an 'acceptable level of risk' means. This may not be a straightforward process, and it may not be possible to set a threshold until after the results of the risk calculation are known.

4.2.1.7 Error reduction / Risk Mitigation

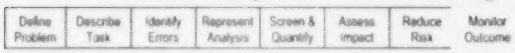


It will be apparent from the preceding sections that a thorough HRA can help to minimise the adverse impact of human actions. However, it will also be apparent that to achieve this effect, the HRA should be undertaken at the earliest stage possible in the design process or the project risks large costs in retrofitting measures to reduce human error to a system that is already constructed. Generally, error reduction strategies include some sort of cost-benefit assessment. The project team will attempt to reduce the level of risk to the acceptable threshold in the most effective manner. There are a number of methods of error reduction and there is a considerable body of knowledge and techniques in the field of ergonomics/human factors (see Table 10 below). Error reduction techniques, at the design stage, can be built into the system. This includes options such as decision support, intuitive interface design approaches, and embedded training techniques, and can also be reflected in different staffing strategies.

Technique	Approach
Reduce error Consequences	Protect the target from potential harm if the event occurs. For example, seat belts in cars, life rafts in ships.
Block Error Paths	Design the system so the error cannot occur in the first place. This may require wholesale functional reorganisation of the system.
Enhance error Detection	Provide improved display systems and associated training. For example, situation awareness displays.
Enhance Error Recovery	Provide more / better options, once error detected, to back track and/or recover. For example, easy to use checklist-based recovery procedures for failures/incidents to ensure that all factors are considered and all necessary actions are taken.
PSF-Based Error Reduction	Identify the effect of PSFs and reduce at source or modify their influence. For example, manage watch (shift) system to reduce fatigue, design interface for fatigued users.
Increase Predictability	Provide improved display systems and associated training. For example, provide feedback to make implications of actions more obvious.
Increase user Control over system	Design control system sensitivity without "hair triggers" i.e. provide buffers or sufficient lag and user feedback to permit users to detect and recover from errors. Match control sensitivity to user skills by through procedures and training. Permit users to customise sensitivity to own skill levels / needs. For example, allow users to customise the level feedback (e.g. novice or expert) depending on the situation.
Increase user Competence	Match user knowledge and skills to more effectively to system demands, through placement, training, organisation and job design. For example, provide embedded on the job training systems as part of system design.

Table 10: Potential Risk Reduction Techniques

4.2.1.8 Quality control/monitoring



For some high risk systems, it may be necessary to convince a regulator that reasonable steps have been taken to ensure the resistance of the new design to human error before operation is permitted – example include nuclear reactors, some industrial processes, and aircraft. To permit the regulator to check and certify the design process, it will be necessary to document how risk was assessed, and the steps taken to mitigate any risks identified.

In the longer term, such documentation can be used to baseline the impact of lifecycle upgrades, manage maintenance and training to minimise risk, to monitor the effectiveness of risk reduction measures and track error probabilities and consequences. The latter is particularly important for the development of error probability data bases for future HRA.

4.2.2 Outline of Some Key models

There are several models in the HF literature that directly or indirectly relevant to analysis of the impact of operator or user behaviour on risk potential, hazard identification, and subsequent risk mitigation.

Some of the most influential models are briefly described below.

4.2.2.1 Skill, Rule, and Knowledge based Behaviour

Rasmussen (1981) developed the very influential Skill-, Rule- and Knowledge-based model based on analysis of human error and prevention in industrial process control settings. Rasmussen's model is based on error reports from power-generation facilities and has been used extensively in HRA to characterise and consider errors.

His model classifies behaviour into three modes.

- **Skill-based** behaviour reacts to stimuli with little conscious effort, as in the case of a well-practised task like changing gear in a car.
- **Rule-based** behaviour involves performance of routine procedures in familiar settings, using memorised or readily available rules.
- **Knowledge-based** behaviour involves event-specific activities that require the person to exhibit higher-level cognitive behaviours such as problem-solving, goal selection and planning.

This model is presented in Figure 9. These categories often overlap, and differences may be subtle. It is sometimes assumed that learning progresses from knowledge to rule to skill based behaviours, though not all behaviours can or do become skill based.

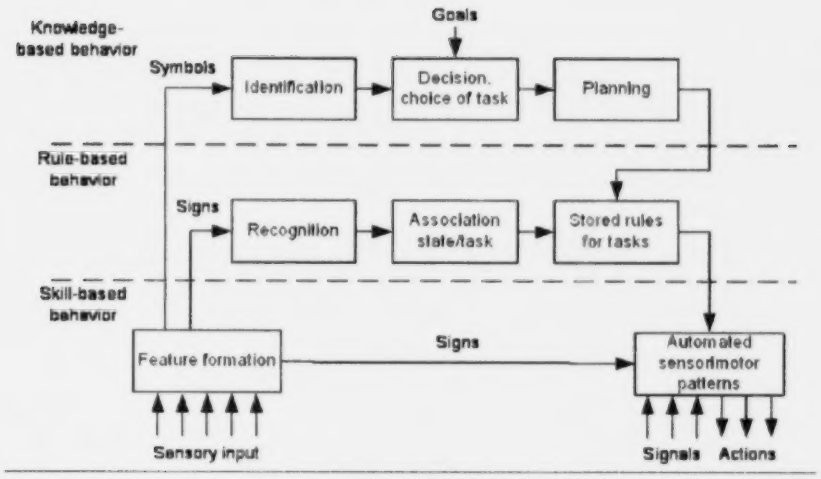


Figure 10: Rasmussen's SRK model

An important concept, present also in other theories, is that of goal orientation. People pursue goals using the behaviours above. Goal formulation and assessment of paths to achieve goals in terms of skill, rule or knowledge based behaviour is a key element and Rasmussen has developed the idea of Decision Ladders to assess how this is done in specific cases.

Figure 11: Rasmussen's Decision Ladder

Subsequent developments such as Ecological Interface Design and Cognitive Work Analysis (Vicente, 1999) emphasise the need to design displays that provide operators with intuitive insight to the relationships among the relevant variables that influence successful control over the process in question. These developments have particular significance for control over complex systems, such as ships, in unfamiliar and infrequent circumstances of which most operators will not have had either direct experience or the opportunity to internalise rule or skill based behaviours.

4.2.2.2 Human Information Processing Theory

Wickens (1992) took earlier characterisations of cognitive behaviours and built the information processing model (see Figure 11). A core component in Wickens model, and of earlier models such as Miller (1957) and Broadbent (1959) is the idea of human beings as limited capacity information processors with constraints on resources such as memory and attention.

There are two important implications of this idea. One implication is that if the limits are exceeded then people will, inevitably, make errors. The type of error will depend on the limitation exceeded: sensory memory, perceptual memory, attention, working memory, response selection, etc (see Figure 11 below). This means that work requirements, displays, task complexity, and decision support aids all need to be considered in the light of such demands if people are to operate effectively in their assigned tasks. No amount of training or size of incentive will get around such limitations in system design.

Another implication is that such resources and their capabilities are negatively affected by Performance Shaping Factors (PSF) such as fatigue and stress. PSFs are particularly important in a multi-tasking environment such as operations on ship's bridge during heavy weather and also need to be taken into account when developing displays, feedback systems and decision support aids.

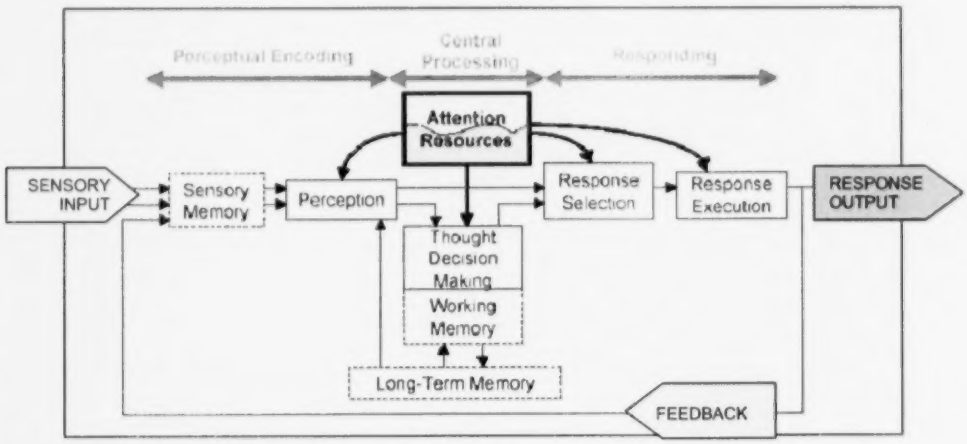


Figure 12: Wickens' Human Information Processing model

Wickens' model has proved to be a robust basis by which to consider human cognition, and can accommodate most, if not all, cognitive activities.

4.2.2.3 Situation Awareness Model

Endsley (1988) took the common sense notion of 'Situation Awareness' and developed a now widely accepted theoretical model, based on research into the challenges facing military pilots flying combat missions. This model has proven effective as a method of considering how a person thinks when doing tasks involving prediction of events in space and time as a precursor to decision making. Endsley's model can also be used to consider human error.

Endsley describes Situation Awareness as having three levels:

> **Level I – Perception** – the individual must be able to detect changes in relevant features in the task environment;
>
> **Level II – Comprehension** – the individual must integrate the identified change into their overall comprehension or "picture" of the situation.
>
> **Level III – Projection** – the individual be able to predict how the "picture" will change if s/he chooses some course of action (including not doing anything).

Endsley's model has been adapted to suit a variety of applications, even though the nature and measurement of Situation Awareness is still the subject of debate. The concept appears particularly relevant for the analysis of ship handling decisions.

4.2.2.4 Domino Theory of Accident Causation

Heinrich (1931) wrote about "The Axioms of Industrial Safety" in which he developed the domino theory. This theory argues that 88% of all accidents are caused by unsafe acts of people, 10% by unsafe actions and 2% by "acts of God". He believed a five-step accident sequence occurred in which each factor would actuate the next step just like we see in a row of falling dominoes. The sequence of accident factors were:

1. ancestry and social environment
2. worker fault
3. unsafe act together with mechanical and physical hazard
4. accident
5. damage or injury.

Heinrich believed that by removing a single domino in the row the sequence would be interrupted, thus preventing the accident. The key domino to be removed from the sequence, according to Heinrich was domino number 3. Heinrich's overall emphasis on worker "fault" is now seen as misdirected and even counter-productive and has been represented as a "*blame the careless worker*" philosophy. However, Heinrich's theory was an important precursor to current theories that incorporate the significance of human behaviour and, as important, the factors that influence behaviour such as interface design, organizational culture, and training.

4.2.2.5 Errors of Omission and Commission

Swain and Guttman (1983) developed a simple but useful error taxonomy as follows:

- **Error of omission** – acts omitted (not carried out);
- **Error of commission** – acts carried out inadequately; or in the wrong sequence; or too early or late. This category also includes errors of quality where an action is carried out to too great or too small an extent or degree, or in the wrong direction, etc.;
- **Extraneous act** – wrong (unrequired) act performed.

Later, Spurgin et al (1987) extended this taxonomy to include:

- **Maintenance testing errors** affecting safety system availability (so-called latent errors);
- **Initiating errors** or operator errors initiating the event/incident;
- **Recovery actions** by which operators can terminate the event/incident;
- **Errors which prolong** or aggravate the situation (e.g. misdiagnosis);
- **Restorative actions** by which operators restore initially unavailable equipment and systems.

This taxonomy is frequently used in HRA.

4.2.2.6 Generic Error Modelling System

Reason (1990) studied the role played by human cognition and behaviour in major industrial accidents such as Bhopal, Chernobyl and Three Mile Island. As part of this work, Reason developed the Generic Error Modeling System (GEMS) from existing models of information processing and existing error taxonomies.

GEMS classifies errors into two categories: slips and lapses; and mistakes. *Slips and lapses* occur at the knowledge-based level, while *mistakes* occur at the rule- and skill-based levels (see Rassmussen SRK model above).

GEMS offers a more useful set of error modes than the SRK model and assigns a variety of errors to each of Rasmussen's behaviour levels (see Table 11 below) to provide compatibility and consistency with the theories on which it is based.

Performance level	Error-shaping factors
Skill-based	Recency and frequency of previous use Environmental control signals Shared schema properties Concurrent plans
Rule-based	Mind-set (*'it's always worked before'*) Availability (*'the first to come is preferred'*) Matching bias (*'like relates to like'*) Oversimplification (e.g. *'halo effect'*) Overconfidence (*'I'm sure I'm right'*)
Knowledge-based	Selectivity (bounded rationality) Working-memory overload (bounded rationality) Out of sight, out of mind (bounded rationality) Thematic 'vagabonding' and 'encysting' Memory prompting/reasoning by analogy Matching bias revisited Incomplete/incorrect mental model

Table 11: Generic Error Modeling System

Reason also proposed the influential '*Swiss Cheese*' model of accident causation (1990). This model suggests that accidents only occur when a number of potentiating pre-conditions align to permit a sequence of cause and effect events to occur (see Figure 12).

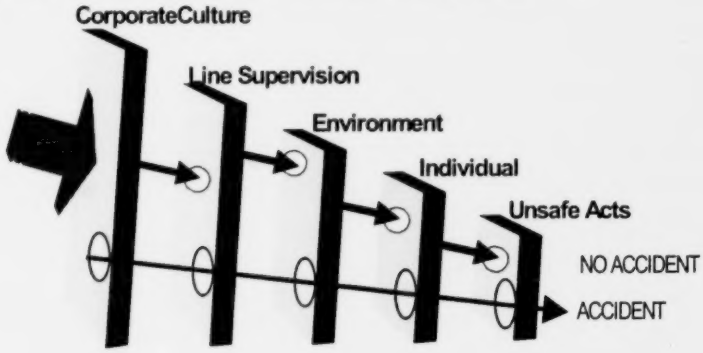


Figure 13: Reason's Barrier Alignment Model

If the potentiating conditions can be identified, this sequence can be interrupted either by inserting barriers, which can be regulatory, organisational, psychological, or engineering, or by changing the nature of the pre-condition itself. For example, if a shift system induces fatigue and error

probabilities are increased by fatigue, change the shift system. Alternatively, if the corporate culture induces risk prone behaviour, change the culture.

However, each of these "barriers" is likely to have weaknesses or holes. If a sequence of events manages to find the holes in each barrier, this will lead to an accident. Some barriers will address latent failures and others will focus on the triggering events at the individual level. The Swiss Cheese model has been widely adopted in a variety of domains, notably aviation where any understanding of human error and accident causation must be demonstrated in order to receive a pilot's license.

This approach has been used by, for example, Harrald et al (1998) to develop organisational (e.g. organisational culture, maintenance, management practices) and operational (decision making, situation awareness, communication) error classifications applicable to maritime operations following the Exxon Valdez incident.

5. Resource Requirements

This section discusses the resources required for HRA and their availability.

A major requirement for any HF work is for the HF analyst to understand the system of interest, task related behaviours within the system, and factors affecting those behaviours. Reliable information needs to come from more than one source and may be acquired by direct observation in the occupational context or a valid simulation, documents such as task descriptions, critical incident reports or training manuals, and interviews or focus groups conducted with experienced Subject Matter Experts. Reliance on a single SME is seldom sufficiently comprehensive or reliable, since the experience and expertise of different SMEs will vary and, inevitably, be selective. This means there is a requirement for access to a cross section of experienced naval SMEs, possibly to suitable simulators, and to data bases of relevant incident reports. Other requirements may include specific modelling or analysis software to calculate probabilities and outcomes of different behaviour patterns, for the sub-system in question.

These requirements are discussed briefly below, together with some available resources.

Direct Observation at Sea

Direct observation / recording of behaviours (combined with interviews) made in the occupational context of interest are commonly a primary source of HF information i.e. at sea during heavy weather. This possibility seems less likely in this case, since the condition of interest, heavy weather, occurs infrequently and unpredictably. Furthermore, access for observers will likely be inconvenient to the navy and costly, even when piggy-backing on other sea-going operations. Thus, direct observation has not been considered further as a practical proposition.

Simulator studies

As a substitute for direct observation at sea, simulator studies have many advantages for the generation of reliable and valid descriptive and quantitative data for identification of error types and estimation of their frequency of occurrence for relevant tasks under simulated conditions. These include the opportunity for multiple runs and to compare behaviours under repeated and controlled conditions. Data capture can also be more effectively managed. However, lack of relevant simulator fidelity may represent a challenge to the validity and generalisation of data to the real world. Furthermore, for reliable quantitative data, there will be need for multiple runs with several suitably experienced subjects. Access to and cost of suitable facilities may also present a challenge since priority is often assigned for training and HF studies are required to piggy back on these. This is seldom satisfactory from the point of view of anything except very general descriptive HF studies.

Simulators are potentially useful for several stages of HRA including task analysis, quantification of effect and probability of different human errors under different sea conditions, researching impact of different performance shaping factors (fatigue, inexperience, etc), and the effects of different risk mitigation strategies (decision support aids, interface designs, training, etc).

Few simulators provide all facilities required for a realistic (and valid) simulator study (e.g. scenario generation capabilities, sufficient fidelity for bridge, sea-state and weather cues, realistic control dynamics in response to operator behaviours, suitable data capture capabilities). Some simulators may only have one, or a combination of several, of the facilities required for a worthwhile simulator study. Thus, it may be necessary for experimental participants to travel to a suitable simulator, or for simulator software to be modified.

It is likely that there are a number of potentially suitable ship's bridge simulators and related software operated by or on behalf of the member nations of the NSSWG. Known resources include:

- **FREDYN wave simulation software.** This software permits complex sea conditions and their interaction with different hull forms to be generated and can be used to drive the RNLN bridge training simulator to provides realistic wave form / hull interactions. FREDYN could possibly be used to drive other bridge training simulators.
- **Bridge training simulators**. Depending on the simulator, these provide varying level of fidelity to train naval officers and other bridge watch-keepers in ship handling, navigation or other bridge related duties. The level of realism depends on the simulator. Known simulators tend to be limited with respect to some visual and auditory and motion cues, such as pounding, wind spray, wind noise, ship motion, etc. It is unknown the degree to which any simulator can be modified to include relevant bridge hardware such as radar, navigation aids, engine room monitors, and prototype decision support mechanisms.

Further investigation is needed to establish what other bridge training simulator resources exist, their capabilities, level of fidelity, adaptability for HRA purposes, and costs of use. Cost of use should include the provision of naval SMEs to act as subjects during the studies, including relevant travel costs to and from the location of a suitable simulator.

Subject Matter Experts (SMEs)

HF studies depend on knowledge of human team organisation and behaviour in the system in question. This inevitably leads to a great dependence on SMEs either in focus groups or individual interviews – sometimes for prolonged periods. Reliance on the experience and opinion of a single SME can be misleading (however well qualified the SME), and reliability and comprehensiveness normally requires data from several SMEs. It is almost a HF truism that two SMEs will seldom agree completely and reliable data is unlikely with a sample of one. The size of the sample (i.e. number of SMEs) required depends on the level of confidence desired.

Working with HF specialists, Naval SMEs will be required for task description and analysis of relevant HF issues for capsize. The MIL report suggests a wide range of potential influences such as ship handling, ship loading (cargo, ballast, etc), engineering changes, and maintenance. This points to a wide range of naval SMEs: bridge watch-keepers experienced in heavy weather operations, engineering officers in ship stability and loading, and naval architects or engineers responsible for initial design and life-cycle upgrades that affect light ship weight and other intrinsic stability issues interacting with ship handling. In addition, for simulator studies of ship handling behaviour, experienced watch keepers would be required to act as subjects.

SMEs will also be required for identification of relevant human reliability issues, assessment of their probability and consequences, and generation of viable risk mitigation strategies and their subsequent assessment. There is likely to be a great number of potential SMEs with the required blend of experience, knowledge and skill, some drawn directly from the NSSWG and the OGWTG. These experts will be an indispensable source of general guidance about the probability of error and the overall risk to a system. However, to avoid the potential for bias in behaviour patterns, participants for systematic simulator trials should be, as far as possible, blind to the purpose of the trial, and represent carefully balanced user profiles in terms of skill and experience. For instance, the reactions of inexperienced users are likely of as much interest as the response of experts.

Scenarios need to be carefully crafted to challenge the participants, with repeated measures and provide for effective data capture.

Access to suitable SMEs is usually limited and needs careful planning and advance bidding for their time. Profile requirements for SMEs will need to be investigated in more detail (relevant experience, qualifications, position or role) as well as their availability and travel related costs in order to make suitable requests for their time.

Data bases

Several forms of data base will be relevant. These include: reports of capsize events and related critical incidents; HF studies of behaviours found to be relevant; the effect of different Performance Shaping Factors; Marine and other incident reports; probabilities of relevant types of human error; the sources and consequences of HF risks for capsize events. Harrald et al (1998) for instance allude to the development of proprietary marine incident reporting systems. A brief search found several relevant data bases (see Appendices), and a more thorough search can be expected to reveal more. Most databases should be readily accessible or obtained, but at an unknown cost. Several considerations need to be investigated further to determine the availability and utility of different data bases for NSSWG purposes. These considerations include: cost, access, format, exportability and compatibility; and type of content

Two reports have been reviewed that represent significant resources. Others undoubtedly exist and deserve more detailed review.

- **MIL stability risk report.**
  This MIL report to DND Canada contains a risk matrix and a fault tree risk evaluation for intact and damaged ship capsize. These represent significant resources and can be used as a point of departure for further Human Reliability Analysis.

- **1944 Typhoon Reports**
  The brief excerpts of these reports available on web sites suggest a rich source of anecdotal data on HF capsize issues. In Admiral Nimitz' summary to the U.S. Pacific fleet following the inquiry alludes to decisions taken by commanders and crew during and before the event, the availability and interpretation of and over-reliance on weather data, awareness of stability characteristics within individual ships, and the need for ship commanders to balance mission directives against ship safety.

Further to these resources, Navies maintain Seamanship Manuals. These will also represent an important data source from which to gather information regarding operator activities and the range of acceptable performance parameters within which these activities are expected to be performed.

Software

Aside from bridge simulator and wave form generation software, two categories of software resource exist.

- One category is network modelling software such as Micro Saint and IPME. Depending on the version used, cost of purchase is approximately $C30,000.00 but should be available as Government Furnished Equipment. However, the costs associated with building the model can be quite significant and far exceed the cost of its purchase. For this reason, areas for such modelling should be carefully chosen and surgically used for areas of high return on investment. But, once broad HF areas of interest are established and prioritised, selective use of such modelling software has high potential utility for task analysis, calculation of baseline outcome probabilities,

and comparison of risk mitigation strategies. Even when applied selectively, the level of effort required for application can still be high.

- The other category of software includes those used for various approaches to HRA. Further investigation is required to establish current availability, utility for NSSWG needs, costs of purchase or use including training required. Non software based approaches do exist.

For all software support requirements, further investigation is needed in terms such cost, utility for NSSWG, and training requirements, validity, and compatibility with statistical analysis support software.

6. Discussion

The NSSWG goal is to establish standards to minimise risks of capsize in naval vessels. While the broad approach to Human Reliability Analysis is well established some development work is required to determine the most effective and efficient approach for capsize issues.

Some of the work still required can proceed in parallel. For example, some problem definition work can go ahead at the same time as further investigation of appropriate databases and facilities required for work further along in the HRA sequence. However, in the first instance, it must be decided how the results of an HRA will be used to identify and reduce HF risks i.e. what sort of standard setting approach NSSWG desires.

- At one extreme, NSSWG could simply require that, as part of ship design, development and subsequent life cycle upgrades, a Human Reliability Analysis should be conducted. In the event that unacceptable human reliability risks are identified, risk mitigation strategies should be determined and adopted. The choices of area of capsize risk to analyse and HRA approach to adopt would be left to the client navy, or even to the contractor.

  This is the approach taken by regulators in some high risk industries, with an audit procedure prior to certification and permission to operate both for the initial design and for life-cycle upgrades. The designer / builder / operator would be required to demonstrate to the satisfaction of the regulator, client, or life cycle manager that Human Reliability risks have been identified and dealt with. If the NSSWG adopts this approach, further HRA work by NSSWG will be used as *guidance* with respect to the HRA process, level of detail and type of output required by the standard.

  This approach would minimise the investment required by the NSSWG and provide flexibility on a case by case basis for the application of HRA to design of different classes of ship.

- At the other end of the spectrum, the NSSWG might undertake a comprehensive (but necessarily generic across different ship classes) HRA for all capsize risk issues and develop appropriate risk mitigation approaches for each area of unacceptable risk. The standard would then direct what features should be incorporated into the design and operation of every ship to deal with those risks.

  This approach would require significant investment by NSSWG. However, it is unlikely that any HRA could cover all types of future ship design; that the risks identified and mitigation approaches stipulated would apply to every type of ship and mission; or that changes in technology over the years might not render specific risk mitigation approaches obsolete.

  The designer / builder / operator would be required to demonstrate to the satisfaction of the regulator, client, or life cycle manager that specific HF risk reduction features have been incorporated into the design of the ship. This approach is *prescriptive* rather than guidance based.

- At an intermediate level, the NSSWG could seek to identify in more detail the HRA approach of choice and conduct studies to establish priority areas (such as within ship

handling and cargo loading) for HRA application during specific ship development and during life cycle upgrades.

The assumption here is that, although ship types differ in construction and intended role, human factors with respect to capsize risk will likely be similar across different platforms. The NSSWG work can identify generic issues of concern to Human Reliability which ship designers and builders can then use as a springboard for Human Reliability analyses specific to the ship type. This should reduce the investment required by the NSSWG and also the costs associated with subsequent HRA because the fundamental HRA issues would only need to be identified once. As with the other approaches, the relevant authority would audit the outcomes in terms of risk identification and mitigation on a ship by ship basis, thus ensuring that safety is fully considered through a combination of previous (NSSWG) work and new work by designer / builder / operator.

This intermediate guidance based approach is recommended as the next step for NSSWG i.e to provide guidance as to the HRA approach to undertake and concerning high priority generic areas for HRA application, while still leaving flexibility for detailed application on a ship by ship basis.

For any of the above options, there are still options to consider for an HRA approach. Choices will vary according to the resources and time available and the criticality of the issue to be addressed.

- **Qualitative vs Quantitative.** One can adopt either a *qualitative* approach based on systematic SME estimates based on a detailed task description, or embark on a more detailed *quantitative* approach that requires access to empirical data for error types and probabilities and the impact of different human Performance Shaping Factors. Not only would the latter be far more expensive but, as far as can be determined, access to reliable and comprehensive PSF data is not available. Generating such PSF data for this or any other similarly complex application is likely unachievable, even with extensive resources in terms of time and money. Thus the recommendation is for an SME based, qualitative HRA approach.
- **Broad vs narrow scope**. A review of the MIL report suggests, even for intact ships, there are at least three areas of high priority for HF: ship handling, ship loading and life cycle light ship weight growth. For the first, the main focus might be bridge watch keepers. For the second, depending on the class of ship, ship engineers and cargo officers. For the third, designers and builders. There is also the interaction between these three categories of personnel to consider. For instance, the degree to which ship's engineers and cargo officers take into account the needs of and communicate with ship handlers – and vice versa. More information is needed to prioritise among these areas and determine the scope of work to be undertaken (see Tasks A and B outlined below).
- **High level vs detailed analysis.** Regardless of the scope chosen, the level of detail to which the analysis is taken is also a choice – for example the degree to which tasks are decomposed and their HF components analysed. This should be an informed choice with greater detail only undertaken for areas identified as high risk and where more diagnostic detail is needed to develop risk mitigation approaches. Initially, it is recommended that analysis should be fairly high level, funnelling down to apply more

detailed analysis once a broad understanding of relative HF risk consequences and probabilities has been gained.

Taken these aspects together, the recommendation is for a broad scope, qualitative approach, with further detailed analysis only as required. Initial problem definition would be based on the existing MIL fault tree in conjunction with a high level task description approach to identify high risk HF areas with reasonable confidence. This would be followed by a decision about what HF issues to consider in more detail (based on a risk matrix approach). A HAZOP involving SMEs would then be used to analyse selected areas in greater detail. For this project, risk mitigation strategies would not be dealt with in detail.

Based on the recommended intermediate guidance based approach, a four task (A-D) work plan is proposed. The four tasks are outlined below with ROM costs (+/- 30%) and set in a time frame of 18 –24 months, depending whether Steps A and Step B are conducted in parallel or sequentially. Costs associated with Step D are where there is the greatest uncertainty since they depend on the scope to be addressed and the costs of the facilities required. However, the scope of work envisioned is unlikely to be achieved for less than the amount estimated especially if the work is to include simulator study and network modelling.

Task A: Extend the existing MIL Systems Fault Tree for intact ship capsize.
Identify likely areas of HF interest and prioritise these for further detailed investigation during Task D. Include the work of other Navies (e.g. the USN) in considering issues related to the risk of capsize. Determine the area(s) to pursue in further detail (see Task C and D)_for the application of HRA. Recommend options for scope of Task D to NSSWG.
Deliverable: Brief report of method and outcome.
The output of this stage will feed into stage B (resource identification) and stage C (detailed planning).
(Time frame: <3-4 months. ROM $15k).

Task B: Further investigation of resource needs and availability.
In parallel with Task A above, investigate marine incident databases, SME availability, simulator facilities and software modelling options (including costs of application) and evaluate suitability of purpose for HRA applications.
Search the technical literature for HF technical articles on capsize related issues e.g. marine incidents that are potential precursors to capsize incidents (based on of the MIL Systems fault tree analysis) – for example cargo loading issues in merchant marine settings, relevant reports of ship handling incidents related to but not culminating in capsize. For instance, the latter could include a more detailed analysis from an HF view point of literature about capsize events e.g. the 1944 Typhoon incident (e.g ballast management, organisational culture issues with respect to the trade-off between mission fulfilment and ship safety), and analysis of ferry capsize incidents. Additionally, information from and about databases and SMEs should be included in these considerations.
Deliverable: Brief report of method and outcome.
The output of this stage will feed into Task C and D by identifying required facilities and their associated costs.
(Time Frame <3-4 months. ROM$15k).

Task C: Prepare a detailed study plan and cost estimate for the area(s) chosen in Task A. Based on Tasks A and B, the plan would detail the task description, analysis and other HRA methods to be used; any network modelling and/or simulator involvement; required SME profiles; travel costs: software use, etc. The plan should also establish clear criteria to evaluate

the outcome of Task D in terms of return on investment to the NSSWG. These criteria might include the following. The range of relevant HF issues identified and their face and content validity; confidence in the risk estimates made. Furthermore, assuming unacceptable HF related risks are identified and that risk mitigation becomes an issue, whether suitable high level risk mitigation strategies can be identified.

Deliverable: Detailed Study Plan.

The output of this stage will be the activities, budget, and schedule for work for Stage D. *(Time Frame <2-3 months. ROM $10k).*

Task D: Conduct the HRA study, report the risk estimate results, including an evaluation of the outcome in terms of the validity and utility of the HRA approach used and any modifications to be undertaken to the approach in future applications to all other HF capsize issues.

Make recommendations for

(a) a HRA approach to identify HF related capsize risks during ship design,

(b) high priority HF risk areas to be addressed during HRA for specific ship designs

(c) High level HF risk mitigation strategies for the HF risk areas identified.

Deliverable: Detailed Report including risk estimates for the HF areas of interest.

(Time Frame 8-12 months. ROM $100 - 150k. depending on scope of simulator / network modelling involved.)

In total, the total cost for this project are estimated to be between CAN$140k and CAN$190k. This can also be seen as the following costs per NSSWG member (i.e. total cost, divided by 7, expressed in Euros, British Pounds, Canadian Dollars, Australian Dollars and US Dollars):

- €12400 - €16800;
- £8900 - £12100;
- CAN$20000 - $28000
- AUS$22600 - $31000;
- US$14600 - $19800.

The table below sets the main work tasks outlined above in the context of the HRA sequence described in the main body of the report i.e. Problem Definition, Task Description, Error Analysis, Error Representation, and Risk Quantification. Risk Mitigation and Outcome Monitoring are outside the scope of this report, but included for the sake of completing the HRA cycle.

Most of these HRA activities fit in tasks A and D (as noted in the table). Tasks B and C (Resource identification and detailed planning) run in parallel with Problem Definition and precede Task Description and subsequent steps in the sequence.

HRA Sequence	Requirement / Potential Approach	Resources required
1. Problem Definition	*Identify focal point(s) for Human Reliability Analysis. (Task A)* Use MIL system fault tree to identify areas for more detailed investigation. Conduct SME focus group to prioritise. Establish capsize scenarios for HRA.	Existing Capsize fault tree(s) Incident data Naval + HF SMEs
2. Task description / analysis	*Undertake task description for priority HF areas (Task A)* Select suitable analysis. Assume Decision Action Diagrams or Tabular Task Analysis. Based on SME interviews and analysis of training manuals. Possibly selective simulator studies to refine task description.	Naval + HF SMEs Bridge Simulator? Cost varies with number & complexity of tasks.
3. Human error analysis	*Analyse tasks for potential for human error (Task D)* Assume HAZOP approach.	Naval + HF SMEs Cost varies with number & complexity of tasks.
4. Representation	*Represent impact of human error. (Task D)* Extend MIL Systems fault tree approach.	Cost varies with number & complexity of HF issues.
5. Quantify risk **6. Establish acceptability**	*Calculate risk. Determine acceptability. (Task D)* Apply enhanced APJ / MIL systems risk matrix approach to quantify risks. Could use network modelling and simulator studies.	Naval + HF SMEs Cost varies with number & complexity of HF issues. Bridge Simulator? Modelling software?
Items below beyond current mandate		
7. Risk mitigation	*Propose and evaluate risk mitigation strategies for unacceptable HF risks* *Depends on outcome of previous tasks.* Evaluate potential using Micro-Saint / IPME / mockups / simulator.	Naval + HF SMEs Cost varies with number & complexity of HF issues. Modelling software Bridge simulator.
8. Set up monitoring system	*Determine system to gather incident data during ship lifecycle(s)* Acquire HF incident data for iterative improvement of / input into future risk assessment. Performance based monitoring of risk mitigation strategies.	Build on current report systems.

Table 12: Plan for Human Reliability Analysis

In every case, existing materials such as the MIL risk analysis should be leveraged for all it can provide, rather than embarking on a new analysis. At the end of the proposed work, NSSWG should have:

- Established, at a high level, significant areas of human reliability for capsize risk,
- Undertaken a detailed investigation to estimate HF related risk probabilities in one or more of those areas,
- Verified the utility and level of effort of the HRA approach adopted, and
- Gained an indication of potential HF risk mitigation strategies, assuming unacceptable risks are identified.

7. Recommendations

The recommendation of this report is that the NSSWG committee adopts a four-step 16- 24 month (depending on scheduling options) study to build on current NSSWG work and resources.

1. Extend the current MIL Systems capsize fault tree analysis into HF issues to select areas for application of the HRA approach.
2. Further investigate the costs and suitability of facilities and other resources (such as SMEs) required for the HRA study.
3. Produce a detailed HRA study plan.
4. Conduct an HRA study in the identified area(s) of interest to provide risk estimates for a range of Human Reliability issues and to validate the HRA process in its application to capsize issues. Based on the outcome of this study, determine the utility of the HRA approach for NSSWG standards requirements and modify as required.

8. References

Broadbent, D E (1958)
Perception and Communications. Pergamon Press, New York.

Endsley, M R (1988)
Design and evaluation for situation awareness enhancement.
Proceedings of the Human Factors Society 32nd Annual Meeting (pp. 97-101).
Santa Monica, CA: Human Factors Society.

Gibson, W.H. (1998)
Development of the CORE-DATA Database in Collection and Classification of Human Reliability Data for Use in Probabilistic Safety Assessments.

Harrald J.R., Mazzuchi T.A., Spahn J., Van Dorp, R., Merrick J., Shrestha S., 1998
Using System Simulation to Model the Impact of Human Error in a Maritime Risk Assessment.
Institute for Crisis, Disaster and Risk Management, George Washington University.

Heinrich, H.W. (1931)
Industrial Accident Prevention. McGraw-Hill: New York.

Kirwan, B I (1994)
A Guide to Practical Human Reliability Assessment. Taylor and Francis, London.

MIL Systems (2001)
CF Ship Stability Risk Assessment SSDMIS - TASK 10. Report No.: 2048-0176-10-01, March.

Miller, G A (1956)
The magical number seven plus or minus two: Some limits on our capacity for processing information. *Psychological Review*, 63, 81-97.

Nimitz C.W. 1945
Pacific Typhoon, 18 December 1944, Admiral Nimitz's Pacific Fleet Confidential Letter on Lessons of Damage in Typhoon. Naval Historical Centre website 2003

Rasmussen, J, (1981)
Models of mental strategies in process plan diagnosis. In J Rasmussen and W Rouse (Eds), *Human Detection and Diagnosis of System Failures*. Plenum, New York..

Reason J (1990)
Human Error. Cambridge University Press, Cambridge.

Spurgin, A J, Lydell, B D, Hannaman, G W, and Lukic, Y (1987)
Human Reliability Assessment, a systematic approach. In *Reliability 87*, NEC Birmingham.

Swain, A D, and Guttman, H E (1983)
A Handbook of Human Reliability Analysis with Emphasis on Nuclear Power Plant Applications.
NUREG/CR-1278, USNRC, Washington DC-20555.

U.S. Navy 1945?
Extracts relating to the Typhoon from the C-in-C's, Pacific Fleet, report. Naval Historical Centre website 2002

Vicente, K J, (1999)
Cognitive Work Analysis - Toward Safe, Productive, and Healthy Computer-Based Work.
Lawrence Erlbaum Associates, Mahwah, New Jersey.

Wickens, C D (1992)
Engineering Psychology and Human Performance (2nd Ed). HarperCollins Publishers, New York.

Annex A: Project Work Tasks

The main tasks stated in the SOW are as follows. Work commenced mid March 2003.

Work Item #1: Project Management

Project management to be kept to the minimum necessary to achieve the objectives of the Statement of Work. Monthly progress reports will be limited to one page outline of progress and problems. Monthly progress meetings will be conducted by phone.

Work Item #2: Develop Outline Plan

2.01: Familiarise with NSSWG work to date.
2.02: Familiarise with broad ship stability issues.
2.03: Identify additional sources of information. Conduct limited key word search.
2.04: Draft outline plan and submit for review by 3rd March.
2.05: Review outline plan with client (phone).
2.06: Revise outline plan based on client feedback.

Work Item #3: Research Detailed Plan

3.01: Conduct detailed review of relevant NSSWG work to date.
3.02: Review readily available sources of further information.
3.03: Review suitability of models of human reliability / error.
3.04: Determine resources / facilities / tools available for implementation of strategic plan.

Work Item #4: Write Detailed Plan

4.01: Draft Strategic Plan and submit draft by 5th May.
4.02: Review with client (phone).
4.03: Revise plan and submit by 2nd June.

Work Item #5: Prepare and Deliver Presentation

5.01: Prepare presentation and review with client (phone).
5.02: Revise presentation.
5.03: Deliver presentation at NSSWG meeting 9th June (Halifax).

Annex B: Supplementary Information

Keywords for Ship Stability

Main Keyword(s) = MARINE/MARITIME/NAVAL/SHIP

Use main keyword in combination with any other keyword(s).
Combine keywords from within a category (e.g. two secondary keywords) to focus hits.

Primary Keywords	Secondary Keywords	Tertiary Keywords
Risk	Probability	Direction
"Human Error"	"Discrete Control Task"	Velocity
"Human Reliability"	"Continuous Control Task"	Bearing
"Performance Shaping Factor"	Judgement	Height
Incident	Ship	"Decision Support"
Hazard	Near Miss	"Data Fusion"
Industry[1]	Method[2]	"Organisational Structure"
"Safety Database"	Analysis	Operator
	Assessment	Training
	Reduction	Simulators[3]
	Mitigation	Outcome
	Barrier	"Centre of gravity"
	Matrix	
	Stability[4]	
	Buoyancy	
	List/Heel	
	"Damage Control[5]"	
	"Situation Awareness[6]"	
	"Task Analysis"	
	"Ship Handling"	
	Seamanship	
	Weather[7]	
	Authors[8]	
	Capsize[9]	

[1] e.g. Offshore, Oil, Chemical, Nuclear, Aviation
[2] e.g. HAZOP, Fault/Event Trees, FMEA, FMECA, Root Cause Analysis, Common Cause Analysis, Probablistic Hazard/Safety/Reliability Analysis
[3] e.g. Modeling [waves, ship motion], Training
[4] e.g. Loading [people, fuel, cargo, ballast], Design/Upgrades, Handling
[5] e.g. Grounding, Collision, Flooding
[6] e.g. Detect, Comprehend, Predict
[7] e.g. Typhoon/Storm/Hurricane/Cyclone, Ice, Tsunami, etc
[8] e.g. Kirwan, Reason, Heinrich, Swain & Guttman, Hale, Kostz [heavy weather ship handling]
[9] e.g. Ferries, Naval, Fishing, Cargo, Container, Oil

National Technical Information Service (NTIS) Search – all documents since 1990

http://www.ntis.gov

Summary of search hit volume.

Marine + "Risk Assessment" = 154 hits (many ecological/pollution related)
Marine + "risk assessment" + human = 30 hits (4 of interest)
Naval + "risk assessment" = 80 hits
Naval + "risk assessment" + human = 12 hits (1 of interest)
Naval + risk + capsize = 4 hits (most by DRE A)
Risk + capsize = 8 hits (most by DRE A)
Naval + "human error" + probability = 1 hit (refers to design process)
Marine + "human error" + probability = 4 hits (1 refers to human errors in loading and discharge)
Seamanship + "human error" = 0 hits
Seamanship = 5 hits
Capsize = 17 hits (included best practices for stability for fishing boats, available in USCG PTP website)
Marine + stability = 200 hits
Marine + stability + human = 8 hits (including 3 sets of proceedings)
Marine + "safety database" + probability = 0 hits
Marine + "safety database" = 0 hits
"safety database" + human = 0 hits
"safety database" = 5 hits (none relevant)
marine + judgement + human = 3 hits (none relevant)
human + judgement + error = 8 hits (3 of interest)
risk + buoyancy = 6 hits (none of interest)
"ship handling" + error = 0 hits
Decision + error + probability = 49 hits (none of interest)
Marine + risk + mitigation = 7 hits (2 of interest)
Marine + "centre of gravity" + risk = 0 hits
Marine + "centre of gravity" = 15 (none of interest)
"centre of gravity" = 428 hits

Other resources found

Journals (Safety Science, Applied Ergonomics, Marine Journals, Insurance Bulletins)
Universities (Strathclyde, Newcastle, Glasgow)
Transportation Safety Board/National Transportation Safety Board/Maritime Accident Investigation Branch
Ocean Ranger (http://www.library.utoronto.ca/robarts/microtext/collection/pages/carylcor.html)
Conferences (ESREL [European Safety & Reliability conference], Human Factors in Ship Design)

URL	General Marine	Guidance	Human Factors	Links	Safety Reports
Washington State Ferry RA.url Risk analysis paper with human element (PWS group)		✓			
ABS Risk Assessment Guidance.url American Bureau of Shipping		✓			
Agency and Salvage Links.url Links from Lloyds shipping agency				✓	
Australian H& S commission.url Statistics about fishing boat capsize					✓
Corrocean Risk Analysis.url Outline of risk analysis and mitigation		✓			
FMEA – Failure Mode and Effect.url Guidance on these techniques		✓			
HSE Marine RA Guidance.url Guidance		✓			
IMO RA Recommendations.url Guidance		✓			
J.Merrick;s Publications.url Part of the PWS group	✓				
Maritime and Coastguard Agency.url Links from the UK MCA				✓	
Prevention through People – about PIP.url USCG (HRA) initiative		✓	✓		
Prince William Sound RA.url Maritime RA group	✓				
Professor Robert G. Bea.url Research into HF of risk in marine systems		✓	✓		
RA for Marine Terminals.url Guidance		✓			
Related links.url Transport Canada links to marine research				✓	
Risk books Risk Assessment and Analysis Website called 'Riskworld' –book list	✓	✓	✓	✓	✓
Safe Marine Transportation (SMART).url University conferences on marine HF			✓		
Safety-Critical (links).url University Glasgow: safety, technique links.				✓	
Seminaire: Maitrise des risques et surete de fonction Methodology and some probabilities		✓			
TAIC Marine Occurrence Abstracts 2000-4 Capsize report from NZ					✓
C TSB Reports – Marine 1996 – M96M0128.url Capsize report from Can					✓
R U Waterloo RA reports.url Risk assessment report from Waterloo		✓			
UK Dept for Transport Marine Accident Investigation Safety digest newsletter					✓

DOCUMENT CONTROL DATA SHEET

1a. PERFORMING AGENCY
Humansystems Incorporated, 111 Farquhar St., 2nd floor, Guelph, ON N1H 3N4

2. SECURITY CLASSIFICATION
UNCLASSIFIED
Unlimited distribution -

1b. PUBLISHING AGENCY
DRDC Toronto

3. TITLE
(U) HUMAN RELIABILITY AND SHIP STABILITY

4. AUTHORS
Robert D.G. Webb; Tabbeus M. Lamoureux

5. DATE OF PUBLICATION
July 4 , 2003

6. NO. OF PAGES
45

7. DESCRIPTIVE NOTES

8. SPONSORING/MONITORING/CONTRACTING/TASKING AGENCY
Sponsoring Agency:
Monitoring Agency: DGMEPM/DMSS
Contracting Agency : DRDC Toronto
Tasking Agency:

9. ORIGINATORS DOCUMENT NO.
Contract Report CR 2003-120

10. CONTRACT GRANT AND/OR PROJECT NO.

11. OTHER DOCUMENT NOS.

12. DOCUMENT RELEASABILITY
Unlimited distribution

13. DOCUMENT ANNOUNCEMENT
Unlimited announcement

14. ABSTRACT

(U) This report briefly reviews ship stability and capsize issues, risk assessment, and Human Factors issues related to risk of capsize during design and operation of warships. A generic approach to Human Reliability Analysis (based on Kirwan 1994) is described in some detail. Based on this approach, a four part two year plan is proposed to establish and apply a Human Reliability Analysis approach to estimate Human Factors risks related to warship capsize and management of stability. This work was conducted under Standing offer W7711-017747/001/TOR, Call-up 7747-14 with DRDC-Toronto and submitted in July 2003.

(U) Le présent rapport examine la stabilité des navires et les problèmes de chavirement, l'évaluation des risques et les questions d'ergonomie liées au risque de chavirement, pendant la conception et l'exploitation des navires de guerre. Une approche générique de l'analyse de la fiabilité humaine (d'après Kirwan, 1994) y est décrite en détail. Cette approche propose un plan de deux ans à quatre volets visant à établir et à appliquer une méthode d'analyse de la fiabilité humaine qui permet d'évaluer les risques ergonomiques liés au chavirement et à la gestion de la stabilité des navires de guerre. Le travail a été accompli en vertu d'une commande (7747-14) passée par RDDC Toronto, subséquente à l'offre à commandes W7711-017747/TOR. Il a été soumis en juillet 2003.

15. KEYWORDS, DESCRIPTORS or IDENTIFIERS

(U) Ship;stability;capsize issues;risk assessment;Human Factors;warships;Human Reliability Analysis